Please return comments NLT 4 August (on the NIPRNET) to both: withersm@ncr.disa.mil and nowakowr@ncr.disa.mil. Comments must be returned by this date to be considered for incorporation in a redrafted TEMP. The draft MDT and OT test plans will be posted by 28 July for comment.

USER REVIEW OF TEMP FOR GCCS V3.0

The attached Test and Evaluation Master Plan for GCCS v3.0, when approved, will provide the agreement among all affected parties for planning, conducting, evaluating, and reporting both DT&E and OT&E in support of the fielding of GCCS v3.0 to replace v2.2.2. This TEMP will be coordinated separately from, but in conjunction with, the GCCS v3.0 EPIP. Although this TEMP describes new capabilities for v3.0, these will be tested and fielded as a second stage, but this draft TEMP does not yet show the planning for this second stage. Also to be incorporated in the next draft of this TEMP will be instructions for planning the testing of subsequent increments to GCCS.

For this round of user review, please concentrate on the following sections and topics:

- Section 1.3, MES: what capabilities must be evaluated in transitioning from GCCS v2.2.2 to v3.0? Remember that the overall criterion is that v3.0 will perform as well or better than v2.2.2, that only 13 known GSPRs will be fixed, and that TPEDIT will replace DART. Note that any MES should be traceable to items addressed in the Requirements Implementation Document, which was sent out with the EPIP.
- Section 1.3, MES, and Table I-1, GCCS Critical Technical Parameters: what specific functions must work and how well, e.g., can you give quantitative minimum acceptable values? If performance is worse than these minimums, testers will come back to you as users to determine whether the mission consequences are acceptable. Consider analogous system performance, experience with v2.2.2, or mission impact as a basis for proposing minimums.
- Section 2.1, schedule. Present schedule doesn't show the details; new schedule will follow.
- Section 2.3, management, lists the roles your organization as well as others are expected to play. These should be reviewed carefully for completeness and supportability. For example, user subject matter experts (SMEs) are needed to support both DT&E and OT&E.
- Section 4.4, Future OT&E: This describes the OT&E focus and any conditions that must be met before or during the OT&E. For example, are there particular databases, interface feeders, scenarios, or events that need to be included?
- Tables 2 through 9 in the "Part IV Appendix" should be reviewed to determine which task(s) are critical to test. Nominate others as necessary, or recommend deletions. Again, what is the minimum necessary to ensure v3.0 will successfully replace v2.2.2?
- Part V, Resource Summary: Although mostly test resources and personnel, it may be necessary to acknowledge your user support in this section.

TEST AND EVALUATION MASTER PLAN (TEMP)
FOR
GLOBAL COMMAND AND CONTROL SYSTEM V3.0

DATE: 21 JULY 1997

PREPARED BY

Program Manager _____ DATE _____

SUBMITTED BY

Program Director _____ DATE _____

CONCURRENCE

Joint Interoperability Test Command _____ DATE _____

User Representative (Joint Staff-J33) _____ DATE _____

OSD APPROVAL

Deputy Director, Operational Test & Evaluation, OSD _____ DATE _____

Deputy Director, Developmental Test Systems Engineering & Evaluation, OSD _____ DATE _____

GLOBAL COMMAND AND CONTROL SYSTEM 3.0
TEST AND EVALUATION MASTER PLAN

TABLE OF CONTENTS

APPENDICES

LIST OF FIGURES

LIST OF TABLES

PART I

SYSTEM INTRODUCTION

1.1 Mission Description

a. This Test and Evaluation Master Plan (TEMP) applies to the Global Command and Control System (GCCS) Version 3.0 capabilities leading up to and including the replacement of the current version of GCCS (Version 2.2). This TEMP will be updated to reflect incremental improvements/upgrades of GCCS.

b. The J3 approved GCCS Mission Needs Statement (MNS) identifies the objectives for GCCS as those identified in the Defense Planning Guidance, Section III, "Command, Control, Communications, Computers, and Intelligence (C4I) and Space Base Systems." Planning guidance for the GCCS is also contained in DODI 4630.8 and the Joint Chiefs of Staff "C4I for the Warrior (C4IFTW)" concept and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01. The GCCS MNS is intended to be one of several MNS within the C4IFTW concept.

c. The GCCS MNS states the required need for selected common functionality among the combatant commands, Services, and agencies which will allow interconnecting to the theater and task force level communications infrastructures. Details of implementation are found in the GCCS Concept of Operations (CONOPS). The mission element need is to provide and support the warfighter with information tools to enable effective and timely accomplishment of the mission. GCCS is an automated tool for the warfighter and supports the primary functional area of C4I. GCCS integrates national, theater, and tactical information into a common, fused picture of the battle space for the warfighter.

d. The Assistant Secretary of Defense, Command, Control, Communications, and Intelligence has approved GCCS as the Command and Control migration system for all the Commanders in Chief (CINCs) and Services/Agencies. The Under Secretary of Defense (Acquisition) terminated the World Wide Military Command and Control System in August 1996, when GCCS became the C2 System Of Record (SOR). GCCS performs not only the many functions of WWMCCS, but also achieves additional functionality required by the Warfighter in a common and interoperable way.

e. GCCS 3.0 will provide the National Command Authorities (NCA) with an infrastructure that will effectively control the flow and processing of information to implement command and control over our national agencies, military forces, and allies throughout the force projection cycle. This capability will extend from the NCA to the CINCs; between the supported and supporting CINCs; from the supported CINC to the Commander Joint Task Force (CJTF); and from the CJTF to the component commands. GCCS 3.0 will enable the warfighter to perform deliberate planning, crisis planning, execution, follow-on operations, and peacetime operations.

1.2 System Threat Assessment

The Joint Staff will conduct the Threat Assessment for the GCCS and provide that document separately.

1.3 Measures of Effectiveness and Suitability (MES)

The Requirements Implementation Document (RID) and the CONOPS constitute the complete requirements documents validated by the Joint Staff. These MESs were used to determine the critical operational issues identified in section IV of this document:

a. Transition from GCCS V2.2. As explained in detail in this plan, GCCS 3.0 will be fielded to a small number of beta sites for Stage III DT and subsequently for OT. In the same manner that the beta sites will utilize GCCS Version 3.0 for testing, transition to GCCS 3.0 for all sites will be accomplished using the same methodology. GCCS Version 3.0 will be backwards compatible with Version 2.2, therefore Version 2.2 sites will point to the new Version 3.0 database (server) using their Version 2.2 software until all of the clients and servers are using Version 3.0 applications. (See paragraph 2.3e)

b. Interoperability. GCCS must interface with Service and site unique systems which pass data to/from GCCS. The GCCS interface requirements draft provided by JITC is found at Appendix B. (See paragraph f(6) below and 2.2c(3))

c. Security. The GCCS shall be accredited to operate at the Secret level during the Security Test and Evaluation portion of the master schedule (Reference CJCSI 6731.01 GCCS Security Policy, the GCCS Automated Information System Security Plan, and associated security documentation).

d. Collaborative Access to a Common Operational Plan. GCCS must support collaboration between the theater-level Joint Operation Planning and Execution Community (JPEC) combatant commands, supported commanders, agencies, Service components, the CJTF and the subunified commander. The specific processes that must be supported include:

- Courses of Action (COA) development
- Forces and task refinement
- Employment analysis
- Specialized employment analysis (e.g., employment of special capabilities that may not currently be in the theater)

- Deployment/transportation analysis
- Sustainment analysis
- On-line refinement teleconferencing
- Remote briefing
- Tailored plan dissemination

e. Visibility of Plan Execution Status. GCCS must provide visibility of plan execution status at all levels of command. At the tactical level, commanders must build a campaign plan from the operational directives given by the CINC. They must be able to access selected resource information from the task force or subunified command components in order to perform resource allocation and task planning/scheduling.

f. Performance. GCCS Version 3.0 system performance must meet or exceed GCCS V2.2 performance standards. Success will be determined by user assessment. The following performance parameters will be measured during developmental and operational testing:

1. Random sampling of functionality using developer provided test plans (in the absence of test plans, individual segment test checklists are developed).

2. Validate system build/upgrade procedures (Solaris, HP, Windows NT)

3. Validate segment installation instructions (Solaris, HP, Windows NT)

4. Validate problem reports are fixed

5. Database Backup/Recovery

6. Service Interface Tests (AFGCCS, AGCCS, MAGTF II)

7. Database Synchronization

g. Reliability (Site). GCCS Site Mean Time Between Operational Mission Failures (MTBOMF) threshold is 82 hours, unless modified by the Joint Staff. MTBOMF is defined as the mean GCCS site operating time between operational mission failures, which cause or could cause the inability to perform one or more GCCS mission essential functions.

GCCS site level MTBOMF will be computed using the standard MTBOMF algorithm defined in AMC PAM 70-11, as follows:

$$\text{MTBOMF} = \frac{\text{Total GCCS Site Operating Hours}}{\text{Total GCCS Site Operational Mission Failures}}$$

where total site operating hours is the sum of fully and partially mission capable operating hours, and total operational mission failures is the total number of GCCS mission essential failure incidents. A mission essential failure includes those incidents where there is no workaround, e.g. the common database is not available, or LAN access to servers is not available, even though the user client workstation is operating.

h. Maintainability. GCCS maintainability is measured at the site level by the Mean Corrective Maintenance Time, referred to in GCCS as Mean Time To Restore software (MTTRsw) and Mean Time To Restore hardware (MTTRhw). The MTTR failures shall not exceed 3 hours for hardware restore actions and 3 hours for software restore actions. These estimates may be revised at a later date and will be based on empirical data. MTTR is the measure of maintainability which describes the average active maintenance time required to complete unscheduled (corrective) maintenance and return a system or component to an operational state after the occurrence of a failure. MTTR is defined as the total active corrective maintenance clock time divided by the total number of corrective maintenance actions performed. Active corrective maintenance time includes the time required to restore all processes, functions, files and databases to a tactically useful state as well as the time to physically reboot the system and enable user logins. Active corrective maintenance time does not include travel time, logistics delay time or administrative delay time. Software failures are defined as any random interruption of the system's operation, other than those directly attributable to hardware, which can be restored to the pre-interrupted state.

GCCS MTTR estimates will be computed for mission operations failures, and hardware and software repair actions, using the MTTR computational algorithm defined in AMC PAM 70-11, as follows:

$$\text{MTTR} = \frac{\text{Total Active Corrective Maintenance Time}}{\text{Total Corrective Maintenance Actions}}$$

where software repair actions are defined as corrective actions taken to restore or reinitialize system operations to the point of processing in progress prior to software module failure. Software repair actions do not include off-line actions taken to revise or update software code.

1.3.1 Availability.

a. The approach for calculating operational availability is defined in the Operational Test Plan, **paragraph 2.2.5** as shown in item b below.

b. Operational availability, Ao, is the measure of system availability that describes the proportion of time a system is operating, or capable of operating, when used in accordance with the system operational mode summary/mission profile in an approved maintenance and logistics support environment. GCCS site Ao estimates will be computed using the following algorithm:

$$\text{Ao} = \frac{\text{Uptime}}{\text{Uptime + Downtime}}$$

Site uptime is time fully mission capable plus time partially mission capable. Site downtime is the sum of the downtime incurred during critical preventive maintenance and the downtime required to restore a site to its pre-failure operating status following mission-critical failures.

Site downtime is composed of active maintenance downtime and associated administrative and logistics downtimes. Site data collection resource limitations preclude independently documenting these downtime categories during the GCCS assessment. However, site downtimes will be

analyzed to identify the factors having the greatest degradation effects on Site Ao. This analysis will identify to the extent possible the site failure modes, maintenance procedures, maintenance deficiencies, and/or supply/support deficiencies which most significantly degrade Ao.

c. In actual practice, the Ao will be expanded to correctly handle the adjudication process in determining the effect on the system when one piece of equipment is down. JITC's actual testing instructions and test analysis will include calculations which take the distributed nature of GCCS into account. In practice, if one component should fail, only that piece will be affected and not necessarily the entire system.

1.4 System Description.

a. GCCS is the primary joint command, control, communications, computer and intelligence systems for the United States Department of Defense (DOD) and provides an integrated architecture of communications and information processing systems capable of responding worldwide to military contingencies throughout the operational continuum. GCCS versions (system and workstation configurations of GCCS compliant software) utilize applications developed by many formal acquisition programs to provide an integrated capability at most levels of command. GCCS is a "system of functionalities" using a common database. It uses a client-server architecture with commercial off-the-shelf (COTS) hardware and a common operating environment (COE) to achieve consistent operation across multiple platforms. Core functions and applications software packages will be selected from migration candidates satisfying selection criteria proposed by the GCCS Program Manager and approved by the GCCS Advisory Board IAW CJCSI 6721.01, Global Command and Control Management Structure and the GCCS Functional Requirements Evaluation Procedures.

b. The GCCS software and hardware configuration along with detailed installation and administration instruction is described in the GCCS version description, GCCS system administration manual and GCCS implementation procedures documents. The configuration identified in the GCCS administration instruction describes the GCCS configuration which will be used for testing. During testing, the configurations of all test sites will be placed under strict configuration management (CM) by the local CM groups and a joint test team composed of both users and testers.

c. The backbone communications for GCCS is the Defense Information System Network. The DISN is a collection of voice and data networks composed of multiplexers, cryptographic devices, routers, and other devices combined to create a world wide information transfer infrastructure. One of the data portions of the DISN is comprised of router based layers,

each with a different classification level. The secret router layer is the Secret Internet Protocol Router network (SIPRNET). The GCCS premise router is part of the GCCS site LAN infrastructure and represents the gateway point out to the SIPRNET Wide area Network (WAN). Communications servers support access to GCCS via Secure Telephone Unit (STU) using dial or dedicated multiplexer circuits.

1.4.1 GCCS 3.0 Functions.

The functionality for GCCS Version 3.0 is described in the GCCS Version Description document (VDD) and was selected in accordance with Chairman, Joint Chiefs of Staff Instruction (CJCSI) 6721.01. The *GCCS User CONOPS* document defines eight objectives for GCCS. These objectives are:

a. Be configurable to achieve optimum crisis response.

b. Support unity of effort and command dominance.

c. Support deliberate and crisis action planning.

d. Provide for joint Time Phased Force Deployment Data (TPFDD) developme

e. Provide Combined Joint Task Force (CJTF) global access to current intelligence and tactical information, in support of joint and coalition missions.

f. Support decision and execution cycles faster than those of the enemy.

g. Provide interoperability for joint and multinational force Command and Control (C2) systems.

h. Facilitate use of Commercial Off The Shelf (COTS) products.

1.4.1.1 FUNCTIONAL CAPABILITIES.

GCCS Version 3.0 will provide the capabilities described in the draft GCCS Version 3.0 CONOPS, sections III and IV, in the GCCS Mission Needs Statement (MNS), and Annex C to the GCCS 3.0 EPIP (Functional Description), 30 May 1997, where specific segment descriptions are found by Solaris, HP, and NT platforms. GCCS capabilities are allocated to four broad functional areas. These functional areas and their respective applications are:

C4I Applications. GCCS C4I applications support a span of control from threat assessment and force requirements development through lift, deployment, sustainment and return. The integration of various intelligence sources and communications links provides the entire GCCS community with the big picture. C4I applications include:

a. **Automated Message Handling System (AMHS)** provides GCCS users with the capability to work with AUTOmated DIgital Network (AUTODIN) messages, both in transmit and receive mode. AMHS also supports the ability to automatically update various databases, based upon formatted AUTODIN messages.

b. **Common Operational Picture (COP)** capabilities are provided by the Joint Maritime Command Information System (JMCIS). Display of near real-time and datalinked air, land and sea tracks are an essential COP feature.

These tracks can be displayed against Defense Mapping Agency (DMA) raster and vector maps.

c. **GCCS Air Tasking Order (ATO) Review Capability (GARC)** provides GCCS with the ability to receive and view US Message Text Format (USMTF) ATO Confirmation (ATOCONF) messages disseminated by the Contingency Theater Automated Planning System (CTAPS).

d. **Joint Deployable Intelligence Support System (JDISS)** is the technical baseline for the DoD Intelligence Information System (DoDIIS) client/ server environment. JDISS includes INTELINK at the Secret classification level. JDISS provides the Joint Intelligence Center (JIC), Joint Task Forces (JTF), and operational commanders with on-site automation support and connectivity to execute the intelligence mission.

e. **Global Reconnaissance Information System (GRIS)** supports the planning and scheduling of monthly theater reconnaissance reports. GRIS is the culmination of migration of three other reconnaissance information systems. GRIS also provides monitoring capabilities.

Planning and Execution Applications. Time Phased Force Deployment Data (TPFDD) is used to develop plans and alternatives, as well as the execution of approved plans. This require the automated tools and activities described below.

a. **Joint Operational Planning and Execution System (JOPES) Navigation (JNAV)** is a graphical system level navigation application that allows users to easily start GCCS applications and switch between them. These include:

(1) **Requirements Development and Analysis (RDA)** allows editing of TPFDDS and graphical analysis of Courses Of Action (COAs) with respect to TPFDD modifications. RDA also provides a capability for creating and modifying force and non-unit requirements associated with Operations Plans (OPLANs).

(2) **Scheduling and Movement (S&M)** handles C2 information on deployment activity and status. S&M tracks and reports on TPFDD requirements. S&M allows GCCS users to work with Transportation Component Command (TCC) carrier and organic movement data before and during deployment. S&M can provide carrier support for more than one OPLAN. S&M allows user Ad Hoc Queries (AHQs).

(3) **Logistics Sustainment Analysis and Feasibility Estimator (LOGSAFE)** uses logistics related attributes, such as unit consumption factors, to calculate time-phased requirements for non-unit related supplies. LOGSAFE can also receive data from Joint Engineer Planning and

Execution System (JEPES) and Medical Planning and Execution System (MEPES). Strategic movement requirements can be grouped to optimize lift needs.

(4) **Joint Flow and Analysis System for Transportation (JFAST)** allows GCCS users to rapidly analyze a COA for deployment and sustainment. JFAST also provides the ability to generate changes to Force Modules.

(5) **Joint Engineer Planning and Execution System (JEPES)** provides GCCS users with a capability to determine requirements and adequacy of engineering support provided in OPLAN COAs. JEPES allows planners to develop the Civil Engineering Support Plan (CESP) for an OPLAN. Using pertinent TPFDD data, JEPES can compute facility requirements and determine if adequate facilities exist to support deployed forces.

(6) **Force Augmentation Planning and Execution System (FAPES)** is a military mobilization decision making tool used to capture and integrate manpower information for deliberate and crisis action planning. FAPES quantifies manpower resources, determines shortfalls and constraints, forecasts time-phased requirements, and monitors mobilization.

(7) **Medical Planning and Execution System (MEPES)** assists the medical planner in quantifying the impact of an OPLAN on the medical system. MEPES can define Medical Working Files (MWF) and compute medical requirements. MEPES also provides data to LOGSAFE.

(8) **Individual Manpower Requirements and Availability System (IMRAS)** supports manpower and personnel decision making planning and execution requirements within each of the JOPES mission areas. IMRAS will support development of the personnel estimate for the situation and personnel appendices to the Joint Strategic Planning System (JSPS) documents.

(9) **Global Status Of Resources and Training System (GSORTS)** is an output application providing status and location of unit data, from the Status Of Resources and Training System (SORTS) database. Unit location can be plotted onto DMA digital map products.

GSORTS currently uses all defined Joint data elements and will eventually contain all Service unique elements. GSORTS allows data retrieval by category of unit, type of unit, specific unit and by OPLAN.

(10) **Ad Hoc Query (AHQ)** is part of S&M. AHQ allows OPLAN end users to query S&M on scheduling and movement requirements for a given OPLAN. A toolkit allows users to build queries and reports, thus minimizing need for specialized knowledge of the database.

(11) **Information Resource Management (IRM)** is a generalized JOPES core database management subsystem. IRM provides the capability to

load, modify, manipulate, and delete OPLAN data. OPLAN access, privileges and auditing are managed through IRM. IRM is also referred to as System Services (SYS SVC).

Mission Support Applications. GCCS, Version 3.0 currently provides three mission support applications, listed below. As the DoD's mission support applications are integrated into the DII, they will become available to GCCS users, as appropriate.

a. **Airfields** provides GCCS users with comprehensive information on over 40,000 free world airfields. This information is supplied by the Defense Mapping Agency Aerospace Center (DMAAC). Reports provide one line summaries for each listed airfield. The database is updated monthly.

b. **Fuel Resource Analysis System (FRAS)** provides planners with an automated capability for determining supportability of a deliberate or crisis action plan. FRAS also generates the time-phased bulk petroleum requirements to support an OPORD. FRAS facilitates the review of fuel requirements for an OPLAN and assessment of adequacy of available resources. Requirements can be generated and analyzed by overall OPLAN, regions within the OPLAN, Service and within a Service by region. Intensity tables and consumption data can be used in requirements generation.

c. **Evacuation File Maintenance and Retrieval System (EVAC)** is a JS and State Department automated computer database and retrieval system used to identify the number of potential evacuees located at each reporting foreign service post worldwide. Retrieval is allowed by country and districts within a country. Information is received from "F77" reports from the AMHS.

Common Operating Environment (COE) Support Applications. COE Support Applications provide four user services, listed below. The primary objective is to furnish, generic, COTS based information transfer services to the GCCS user community and their applications.

a. **Office Automation** is supported by a suite of Applixware COTS products, including Applix Words, Applix Spreadsheets, Applix Mail, Applix Power Brief and Applix Ovation. The latter is a presentation application that communicates with DOS based systems.

b. **Teleconferencing (TLCF)** Two applications provide GCCS users with teleconferencing functions. A third application provides a World Wide Web information search and retrieval capability.

(1) **Internet Relay Chat (IRC)** is a chatter style application that allows multiple users to participate in conferences. Several types of channels, with varying degrees of privacy, can be established.

(2) **Internet News** provides access to a bulletin board style broadcast service. Articles posted to the bulletin board are arranged by newsgroups. Various functions are supported, including the ability to trace a subject through a series of articles within a newsgroup and send correspondence to article authors.

(3) **World Wide Web (WWW)** browser service is provided through Netscape. The GCCS user may retrieve information through queries or links to other documents or websites.

c. **TELNET** provides the GCCS user with the ability to log-in and use the application resources of any server across the network. The principal function of TELNET is to initiate text based or X-Windows applications, which, because of application design or security, must be executed from a specific server instead of from the user's local hardware.

d. **File Transfer Protocol (FTP)** is used to directly control the transfer of files to and from a distant server. FTP is especially useful in transferring large files and is recommended when e-mail attachments exceed 500K bytes.

1.5 Critical Technical Parameters

The GCCS contains several software components which support a broad user base. The GCCS critical technical parameters were derived from the GCCS MNS, CONOPS, and related system documentation and are provided in Table I-1. Specific performance requirements for the components of GCCS will be application specific. These parameters will be refined as specific site usage and requirements are available.

Table I-1. GCCS Critical Technical Parameters

Critical Technical Parameter	Technical Objective/ Threshold	Total Events	Location	Schedule	Decision Supported
Interoperability Certification	Must obtain interoperability certification. Must verify compliance with the certified GCCS IT standards profile which must contain applicable standards in the DoD TAFIM	GCCS version 2.2	MDT at Executive Agent Multi-node Test User Assessment OT	See Fig 2-1	GCCS V3.0 Fielding
Site MTBOMF	82 hours*	As Above	User pre-assessment User assessment OT	See Fig 2-1	GCCS V3.0 Fielding
SW reliability --Priority 1 SIR	Only Joint Staff approved Priority 1 or 2 GSPR	As Above	MDT at Executive Agent, OSF User pre-assessment User assessment Multi-Node Test OT	See Fig 2-1	GCCS V3.0 Fielding
Maintainability (Software) Site MTTRsw=Mean Time to Restore	3 Hours*	As Above	User pre-assessment User assessment OT	See Fig 2-1	GCCS V3.0 Fielding
Maintainability (Hardware) Site MTTRhw = Mean Time to Restore	3 Hours*	As Above	User pre-assessment User assessment OT	See Fig 2-1	GCCS V3.0 Fielding
Site-level Availability Ao	95%*	As Above	User pre-assessment User assessment Multi-Node Test OT	See Fig 2-1	GCCS V3.0 Fielding

*May be revised based on empirical data.

PART II

INTEGRATED TEST PROGRAM SUMMARY

2.1 Integrated Test Program Schedule.

This section identifies overall responsibilities for managing, conducting and coordinating GCCS test activities. Figure 2.1 identifies the key events and activities to support the testing, evaluation, and fielding of GCCS Version 3.0. The GCCS Program Management Plan describes a time-staged implementation approach for overall GCCS program management and implementation. The GCCS test and evaluation strategy is designed to leverage the development efforts of a large number of programs. Each program may have several development organizations. GCCS includes the integration of CINC and Service-unique feeder applications which must be integrated before GCCS user exercises can be run. In addition, new applications will be integrated as they become available. GCCS will employ an incremental integration, test and fielding approach. Target application requirements identified by the functional proponent will be segmented, tested, and fielded. The T&E strategy will utilize developmental and operational test and evaluation methods described in sections three and four respectively. MDT&E will be performed by the designated development agencies (DDA), the DISA integration test team, and the independent developmental testers and users. See Figure 2.1.

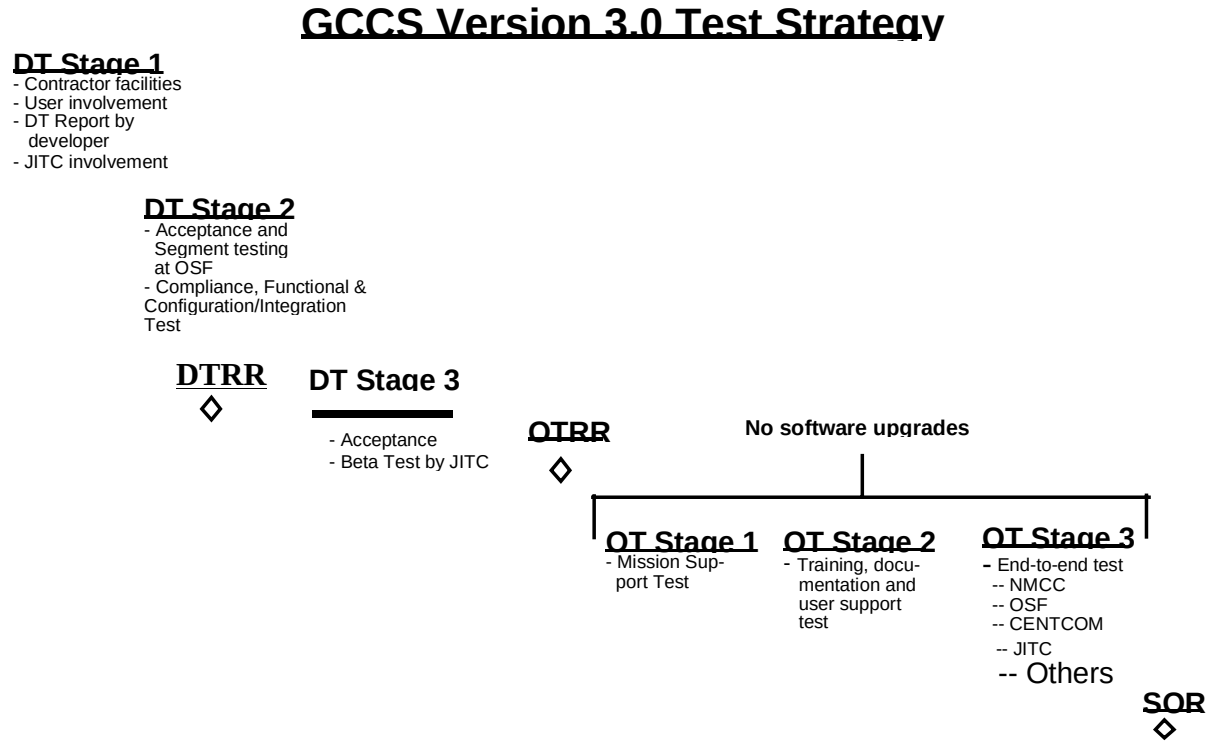

Figure II-1 GCCS Program Schedule

a. Developmental Test & Evaluation. A Modified Developmental Test approach will be used for GCCS Version 3.0 that includes the stages described below:

DT Stage 1 will be conducted at the developer's facilities. The GCCS users will assist the contractor in evaluating the functionality with demonstrations and testing before delivery. JITC will provide oversight and will provide reports during this testing to the GCCS Program Office. The developer will provide a DT Report prior to delivery of the components to the Operational Support Facility in the formal segment delivery process.

DT Stage 2 will be conducted at the Operational Support Facility. This Stage will include compliance, functional and configuration/integration testing of the initial component deliveries. System builds and installation instructions will be validated. Software problem reports (GSPR) fixes will also be validated in Stage 2.

DT Stage 3 will be led by the JITC and consist of a beta test with user involvement and acceptance as part of OT Readiness Review.

b. Operational Test & Evaluation. OT&E will be performed by the JITC in conjunction with the Service test agencies (AFOTEC, OPTEC/OEC, OPTEVFOR, MCOTEA). Operational assessments of the earlier versions of GCCS were conducted by the user community under the auspices of the Joint Staff (J3). Additional assessments of CINC and Service unique applications integrated into GCCS 3.0 will be performed by the providing CINC or Service, and supplemented by independent operational tests. An OTRR will be convened to determine the suitability of the system to enter operational testing. The OTRR will establish the 3.0 baseline. Once OT has commenced, no major software changes will be permitted without returning to DT. The stages of the OT are described below:

OT Stage 1, Mission Support Test. JITC will conduct the Mission Support Test at multiple operational sites. Test sites for Stage 1 will be a subset of the sites for Stage 3. The objective is to determine if mission support personnel (for example, system administrators, database administrators, network administrators, security personnel) can install and configure the system, establish user permissions, establish network connectivity, establish security controls, and otherwise prepare the system for effective operation. The GCCS user community will provide subject matter experts (SMEs) to support assessment of Mission Support task success.

OT Stage 2, Assessment of training, documentation and user support. This stage will not include test activities. JITC will review the training program, system documentation, and procedures for user support. JITC may support the assessment by administering questionnaires to selected user personnel. The objective is to determine if the training is adequate to prepare the users to perform their missions, if the documentation is adequate for use by operational personnel, and if the user support structure (for example, help desk) is adequate for operational use.

OT Stage 3, Simulated Crisis Situation. JITC will conduct this test at multiple operational sites (and, possibly, one or more lab sites). Functionally, the sites will represent a supported CINC, one or more supporting CINCs (including TRANSCOM), the NMCC, a JTF headquarters (austere environment), and an afloat headquarters. Actual sites may include EUCOM,

CENTCOM, PACOM, TRANSCOM, NMCC, ACOM, CENTCOM, SOCOM, JITC lab, OSF. Actual users will operate the system at all sites (including any lab sites). The GCCS user community will provide subject matter experts (SMEs) to support assessment of Mission Task success.

2.1.1 Critical System Milestones.

The following aspects of the GCCS may present special test and evaluation requirements:

a. Database Synchronization. Maintaining synchronization of the JOPES core database content across database sites in a operational environment will be evaluated.

b. Essential applications. Several new or enhanced functionalities are planned for GCCS Version 3.0. They include but are not limited to the following:

1) JPET. Deliberate/crisis planning tools
2) MIG
3) METOC
4) JFRG
5) C2PC
6) DII COE V3.1

These applications will be included as software segments, ready for use without requiring patches. Software should not contain Category I or II discrepancies in critical errors, as defined in the Evolutionary Phased Implementation Plan (EPIP), unless approved by flag level at the Joint Staff. The most current GCCS 3.0 build list of segments is provided in Appendix D.

c. Robust GCCS network should exist with the following:

1) All SOR hardware installed/operational
2) SIPRNET certified SECRET NOFORN
3) SIPRNET connectivity among SOR sites achieved
4) Network management policy in place
5) Functional network plan in place (includes remote backup database locations and local database recovery procedures
6) CINC/Service specific hardware/software tested and in place
7) Successful multi-node database synchronization checked
8) AMHS functions available

d. Sufficient written procedures and documentation available to the user including-

1) Application user manuals
2) Training manuals (for system, security, database, and network administrators)
3) Integrated Logistics Support Plan (ILSP)
4) Administrative Documents (EPIP, Operational Test Plan, and CONOPS)

2.2 Management.
Management responsibilities for the GCCS program are as follows:

a. DOT&E. Responsible for the final approval of coordinated TEMP and OTP. Also responsible for the oversight of test planning and conduct and independent evaluation and reporting of GCCS performance.

b. DTSE&E. Reviews development test results to analyze residual risks and satisfaction of entrance criteria.

c. Joint Staff. Responsible for the following activities:

(1) The specification and approval of operational requirements.

(2) Conducting a threat assessment for GCCS.

(3) Approving exit criteria at each stage of DT.

(4) Providing user and/or SME support as necessary.

(5) Validating any modifications or interpretations of the user requirements. This may require approving changes to the operational requirements.

(6) Final approval authority for the operational use of GCCS Ver 3.0.

(7) Providing test scenarios as needed.

(8) Represent the CINCs for the TEMP and OTP.

(9) Establish Concept of Operations (CONOPS).

d. The GCCS Program Management Office (PMO) has responsibilities for the following activities:

(1) Ensuring testers and users have access to developer facilities, products and data.

(2) Ensuring DT and OT efforts are adequately resourced (in a timely manner).

(3) Interfacing with the Joint Staff and Service users to ensure all valid requirements are considered.

(4) Resolving conflicts between user and developer, if any. This specifically addresses contract deliverables and meeting user requirements.

(5) Completing and coordinating the TEMP.

e. DISA/JIEO/OSF. Responsible for the following activities:

(1) Complete the description of the transition strategy options for fielding and backing up the GCCS both before and after GCCS v3.0 SOR. DISA will provide version description documents, system administration procedures and a cutover plan for the database and long haul communications.

(2) Provide baseline and developmentally tested software and related support to GCCS fielding sites.

(3) Complete the development test of the DII Common Operating Environment (COE).

(4) Ensure the capability to restore GCCS Ver 2.2 to full operation.

(5) Validating installation procedures as defined in the engineering strategy.

(6) Validating COE compliance and providing results to developer.

(7) Testing baseline software and providing emerging results.

(8) Using applicable metrics to evaluate the status of the system.

(9) Providing overall system status reports in coordination with the JITC.

(10) Participating in Stage 3 as a supporting test node.

(11) Retesting GSPRs and providing results.

f. Services. Responsible for the following activities:

(1) The specification and approval of the operational requirements and operational procedures for Service unique elements of GCCS

(2) Conduct operational test and evaluation for GCCS Service Interfaces and Service unique mission critical capabilities in support of the OTP and appended Service test plans. Operational test support includes writing test plans, test execution, evaluating test results and providing the evaluation of operational effectiveness and suitability to JITC for consolidation into the overall GCCS evaluation. This will allow JITC to monitor Service unique testing prior to System of Record (SOR).

(3) Provide GCCS Ver 3.0 cut-over recommendations to JCS/J3.

g. JITC. Responsible for the following activities:

(1) Establishing an Independent DT team.

(2) Identifying and verifying testable GCCS 3.0 requirements.

(3) Recommending applicable software metrics for GCCS 3.0.

(4) Coordinating input to test documentation for DT stages 1 and 2.

(5) Producing test documentation for DT stage 3.

(6) Coordinating with Joint Staff, GCCS user working groups, and Service communities to ensure user interest.

(7) Recommending areas for SME assessments/involvement.

(8) Reviewing applicable system documentation.

(9) Providing emerging results reports as applicable and providing a system status report at the end of each stage of testing.

(10) Developing the test scenario for DT Stage 3.

(11) Providing anomaly reports.

(12) Providing requirements assessment.

(13) Providing MDT&E report with recommendations.

(14) Interfacing and coordinating with DISA security personnel for GCCS security issues.

(15) Drafting appropriate exit criteria.

(16) Coordinating with the PMO to produce Part III of the TEMP.

(17) Providing input to Parts II and IV of the TEMP.

(18) Independent operational testing.

(19) Interoperability testing and certification, to include Y2K testing.

(20) Coordination with Service test communities to leverage test planning, conduct, and evaluation of Service-unique critical mission tasks.

(21) Coordinate user involvement at the contractor facilities for the purpose of

operational assessment.

(22) Site installation evaluation.

(23) Consolidating the reporting of entrance criteria requirements.

(24) Writing the Operational Test Plan (OPT) and serving as the single operational test integration point of contact.

(25) Test training and coordination.

(26) Control over the GCCS configuration during the operational stage of testing, and control over access by contractors that might alter the configuration.

(27) Ensure that all mission critical tasks are performed and evaluated, or that the consequences of not performing any critical mission are assessed by the affected users as an acceptable risk and test limitation.

(28) Consolidate evaluation reports from appropriate sources; conduct, analyze, and evaluate the joint portion of GCCS operational testing; and reporting test results directly and simultaneously to the Joint Staff, Director of DISA, and DOT&E with information to the Services.

h. CINCs, Services and Subject Matter Experts (SMEs). Responsible for the following activities:

(1) Providing experienced and knowledgeable user representatives as the designated SME - the primary interface for specific GCCS components/ applications.

(2) Monitoring Newsgroups that are announcing problem report fixes.

(3) Responding to scheduled opportunities to visit developers and to participate in user demonstrations of their designated GCCS components/applications.

(4) Providing input to the DT and OT teams to help develop appropriate software metrics for their specific GCCS component/application.

(5) Reviewing plans for and participating in the integration, configuration, and systems tests conducted at the OSF.

(6) Reviewing plans for and participating in the network and systems tests conducted at designated Beta test sites, the JITC, or the JDEF.

2.3 **Procedures**

a. Adjudication. Problems identified by exception during testing will be adjudicated by on-site teams consisting of users and administration personnel as selected by the sites. The adjudication process compensates for a lack of required performance standards and allows users to determine criticality of incidents. During designated test periods, the adjudication process will determine scoring of test incidents prior to forwarding the test incidents to the JITC for collection and analysis. Certain categories of problems will require the submission of both the test incident form as well as a GCCS System Problem Report (GSPR) through established channels to the Program Manager. In these cases, the test incidents form will include a cross-reference to the GSPR submission.

b. Test Independence. The test team members must be independent from the system developers and integrators. Test results need to be consolidated and reported through independent channels rather than user or developer channels. Users in the test must be able to express themselves freely.

PART III

MODIFIED DEVELOPMENTAL TEST AND EVALUATION

3.1 Modified Developmental Test and Evaluation (MDT&E) Overview

The MDT&E effort for GCCS will verify the status of engineering development progress within each segment, verify that design risks have been minimized, substantiate achievement of technical performance requirements, measure the effectiveness of the functional requirements and certify readiness for operational test (OT) through use of SW Metrics and DT results and analysis.

a. DT&E Test Philosophy. GCCS will use a modified MDT&E test philosophy that incorporates the following concepts:

(1) Stronger user involvement. Early involvement from the user community is the key to a successful DT approach. Working closely between the developers and user community in developing GCCS capabilities helps ensure user requirements are met and capabilities can be evaluated in a user-oriented environment.

(2) Extensive use of existing software. GCCS will integrate a wide assortment of software systems that interface in a standard way with the DII COE. The applications to be integrated include existing command and control systems, and systems created and used by the Services. One of the goals of GCCS is to fully integrate selected Service applications that use the DII COE, to avoid large and lengthy development efforts.

(3) Use of event driven scenarios based on requirements as a means of evaluating the effectiveness of GCCS products and application software in a user-oriented environment.

(4) Use of exercise-like scenarios during end-to-end testing to evaluate the effectiveness of the multi-node environment and benchmark the thresholds of the system. New versions will be at least as capable in performance as the version replaced.

(5) Customizing the test and evaluation process according to segment type and the magnitude of the risk involved with inserting the segment into the operational GCCS system. Because the GCCS is made up of applications developed by each of the Service components, as well as COTS software, the testing completed by the development activity will be factored into the independent MDT&E activities.

(6) Use standard SW Metrics throughout the development effort to measure the growth and stability of the GCCS system. These metrics will provide a portion of the entrance criteria into the OT&E effort as well as provide a "snap shot" of the current status of the GCCS system.

(7) Ensure that the OT&E interests are considered during MDT&E events to include the participation of the OT&E community at DT planning events, DT events and DT analysis and reporting efforts.

(8) Use of development test data by the operational test community as preliminary operational data for input into their assessments supporting GCCS Version 3.0 determination of operational effectiveness and suitability and minimizing the need for collecting data multiple times.

b. DISA Developmental Test and Evaluation Methodology. The objectives of DISA developmental test and evaluation for GCCS are to reduce the risk of adverse impacts when inserting new segments and technology into the operational system, and determine the effectiveness and supportability of the component in a user-oriented environment. DISA will oversee and conduct DT for the GCCS Version 3.0 development and integration effort prior to Operational Test and Evaluation (OT&E) efforts. The MDT&E methodology incorporating the MDT&E philosophy into a three staged DT approach is depicted in Figure III-1 below and detailed in subsequent paragraphs within this section. The following paragraphs describe the MDT&E methodology for GCCS version 3.0. Table III-1 list the exit criteria for each of the three DT stages and Table III-2 list the products for each stage of DT.

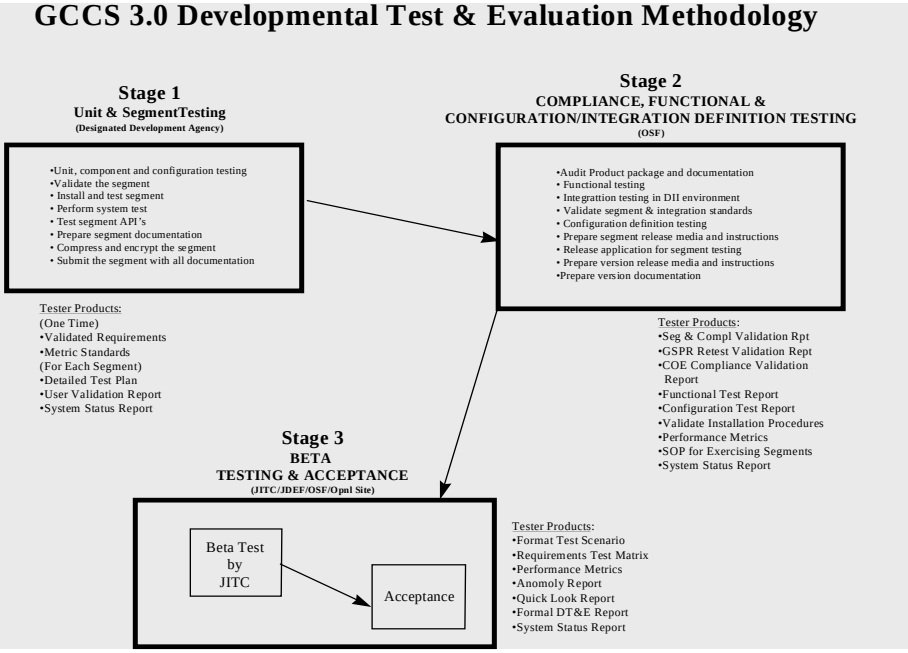

Figure. III-1. GCCS 3.0 Developmental Test & Evaluation Methodology

(1) **Application and Segment Testing**. Stage 1 encompasses Unit and Segment Testing conducted at the developer's facilities. The segments or units will be developed and documented in accordance with MIL-STD-498, the segments shall be validated with their appropriate platform COE and user participation for applicable segments will be required. JITC will provide oversight and guidance to the developer to ensure exit criteria, shown in Table III-1 from Stage 1 has been met and SW Metrics are captured to effectively measure Stage 1 events.

Table III-1. MDT&E Exit Criteria

Stage 1 **Application & Segment Testing**	Stage 2 **Compliance and Integration Testing**	Stage 3 **MDT System Testing**
Application functionality verified at developer facility	Application functionality verified at Government facility	Application/System functionality verified at lab and operational sites
Priority GSPRs fixed, adequate workaround documented, or program decision on GSPR is made.	Scheduled GSPR fixes are validated in lab; OSF integration and unit testing performed	Scheduled GSPR fixes validated by user
	Segments are Validated for Compliance DII COE in lab	Installation instructions are verified by user
	Installation Instructions are verified in lab	Interfaces Validated by user

a. The Designated Development Agency (DDA) for all segments and major configuration items will complete a Formal Qualification Testing (FQT) process in accordance with MIL-STD 498 during unit and segment testing. A Software Test Plan (STP) will document the developer's plans for conducting FQT. The developer will define a preliminary set of engineering requirements for each computer software configuration item (CSCI). As part of FQT, the developer will define a preliminary set of qualification requirements for each CSCI. These requirements, to be documented in the preliminary Software Requirements Specification (SRS) for each CSCI, are to be consistent with the qualification requirements defined in the system specification. The developer will identify and describe the test cases for each FQT in the software test description (STD) for each CSCI.

b. FQT will consist of unit, component and configuration item testing. Unit testing ensures the component algorithms and logic employed by each unit are correct and that the unit satisfies its specified requirement. Component testing ensures that the component algorithms and logic are correct, that they satisfy the specified requirements and that the subordinate components and units are integrated properly. Configuration items testing ensures that the entire program operates according to design specifications.

c. Throughout the Stage 1 process the development proponent/users will be involved as both observers and commentators on the test results. The schedule and location for development proponent/user participation will be dependent on specific segment and application development.

d. The DDA will then deliver the software to the government upon satisfactory completion of FQT in accordance with MIL-STD 498, and per guidance contained in the Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS), Version 3.0, Specification/Draft, dated 1 January, 1997. Satisfactory completion of this testing is a prerequisite for the subsequent testing stages.

(2) **Compliance, Functional, and Configuration Definition/Integration Testing.** Stage 2 includes Compliance, Functional and Configuration Definition Integration Testing. All GSPR's are re-tested and validated as corrected or returned. All segments are verified as complete and integrated into the GCCS version. Installation instructions and system documentation is developed and verified. Users will participate in or witness testing of selected GCCS V3.0 capabilities in this stage. JITC will provide oversight and guidance to JIEO to ensure that the exit criteria for Stage 2 has been met and software metrics are captured to effectively measure Stage 2 events.

a. Compliance Testing. Segments will be delivered to the GCCS program in accordance with the GCCS Configuration Management (CM) Delivery Letter. All segments will have been functionally proven/accepted by development proponent prior to delivery to the GCCS program. All segments to include selected COTS and GOTS software components proposed for integration into the core system will be compliance tested in accordance with the DII I&RTS (low level integration with COE & associated segment) to ensure that they have been integrated with the COE and that they work with associated segments in the COE and do not damage the environment. A compliance checklist extracted from the I&RTS is utilized to validate each segment.

b. Individual Segment Functional Testing. Random sampling of the individual segment functionality using developer provided test plans will be tested. In the absence of test plans, individual segment test checklists and procedures will be developed. The functional testing also includes validation of the system build/upgrade procedures (Solaris, HP, and NT), validation of segment installation instructions (Solaris, HP, and NT), validation of problem reports/fixes, and backward compatibility between versions.

c. Configuration Definition/Integration Testing. Configuration Definition testing involves integrating CSCIs with interfacing hardware configuration items (HWCI) and CSCIs, evaluating the resulting groupings to determine whether they work together as intended, and continuing this process until all CSCIs and HWCIs in the system are integrated and evaluated. It is designed to verify the proper integration of the configuration items with each other, and with the system environment. This process is designed to test the critical functionality of a critical mass of applications after integration with a GCCS version. This testing includes validating interfaces with Service and CINC applications migrating to or coexisting with GCCS. The testing will be performed in a lab environment at the OSF. Multiple GCCS nodes (a nodes includes a database server, application servers, and client workstations) will be utilized during this stage to validate database synchronization and system interfaces across a simulated wide area network.

(3) **MDT/System Testing.** Stage III consists of conducting application and system testing, at selected MDT sites, to verify integration and functionality, lead to a recommendation on acceptance, and prepare for an Operational Test Readiness Review (OTRR) with full user involvement. Users will evaluate if the functional and technical user requirements are met. Interfaces with feeder systems, when made available, will be evaluated. Priority 1 & 2 GSPR fixes, that were not validated in previous stages, will be validated. Some GCCS application functions will be selected for inclusion into the Performance Characterization effort. The Performance Characterization effort will test, track, and record application response times during testing. Performance Characterization data can be later used by operational sites as a rough yardstick for planning and comparison purposes of their GCCS suites. JITC, working with user Subject Matter Experts (SMEs), will ensure that the exit criteria for Stage III have been met and that the results provide enough data to facilitate an OTRR decision.

a. During this stage, JITC will work with users and verify the installation procedures and software load programs for each available platform type. The MDT sites will use the procedures in the GCCS Version 3.0 release notes to produce the system. The MDT sites are JITC lab at Huachuca, JITC lab at JDEF, and some operational sites that are to be determined. The certified/accredited security features and procedures will be in place. Representative System Administrator, Network Manager, Security Manager, and Database Managers will validate their procedures. The

IDTA will document any abnormalities. DISA will either fix the problem or revise the installation procedures to document the error/workaround. The testing will validate that the mission specific software performs as designed under realistic operational constraints. The test will exercise the system in a multinode environment. This will serve to validate the Wide Area Network (WAN) configuration. Using the provided user level documentation, the users will, with the aid of the JITC test team, evaluate the systems capabilities as defined in the requirements document at the test locations, exchanging representative data.

b. Service feeder systems and site unique systems, whenever available at the MDT sites, will be included in this stage's testing. Their interoperability with GCCS will be evaluated. OT&E team members will be involved at this stage as independent observers for data collection purposes in preparation for subsequent OT activities. Service feeder systems not available during this stage, can be evaluated for interoperability with GCCS during the OT&E.

c. Results. Shortly after completion of this stage, a "Quick Look" report will be generated to summarize the results. The formal MDT Stage III report detailing all the results will be published within a few weeks of this stage's completion. Both reports will include the results of the performance characterization of selected GCCS functionalities. Both reports will be provided to the developer, user, and operational tester as support documentation at the OTRR.

Table III-2. MDT PRODUCTS

STAGE 1		STAGE 2		STAGE 3	
IDTA	**OTHER AGENCY**	**IDTA**	**OTHER AGENCY**	**IDTA**	**OTHER AGENCY**
Requirements Baseline	Delivery Letter	Segment & Compliance Validation Report	SW Version Description	Formal Test Scenario (including test events	Final Accreditation
Metric Standards	List COTS License	GSPR Validation Report (Re-Test)	IATO or Final		
Detailed Test Plan*	Version Description Document	COE Compliance Validation Report	STE	Performance Characterization	
Software Test Plan*	System Requirements Specification	Functional Test Report	Interface Design Document	Anomaly Report	
Software Test Description	Database Design Document	Configuration Test Report		Quick Look Report	
User Validation Report	Installation Procedures	Installation Procedures*		- Emerging Results	
System Status Report	Software Test Plan	Performance Metrics*		Formal MDT&E Report	
	Software Test Description	SOP for Exercising Segments		System Status Report	
	Operators Manual	System Status Report			
	System Administrators Manual				
	System Users Manual				
	Segment Description (Output)				
	Segment Abstract				
	Release Restriction Instructions				
	Segment or Patch List				
	Performance Metrics				
	Security Plan				
	Collected Metrics				
	Interface Design Document for Various Interfaces				

*** Input/comments only. Note: Some reports may be combined**

c. Test Facilities. Test facilities being used to test the GCCS include the JITC test bed at Fort Huachuca, AZ; the Joint Demonstration and Evaluation Facility (JDEF) in Arlington, VA; the Operational Support Facility (OSF) in Sterling, VA; and operational sites TBD. Each of these facilities will include GCCS operating platforms, software, and communications equipment necessary to operate as an operational GCCS site and will have remote access to the various CINC and Component GCCS sites worldwide. Thus, each facility will be able to support test case development, system performance analysis, joint exercises, GCCS user workshops, and other system demonstrations. These facilities provide an excellent capability to balance testing done in laboratory and operational environments.

3.2 Developmental Test And Evaluation to Date

GCCS Versions 1.1, 2.0, 2.1, and 2.2 have been installed along with the GCCS hardware environment consisting of open system servers, workstations, and COTS capabilities.

a. Version 1.1 included the initial release of the Common Operating Environment (COE) upon which future development efforts were based.

b. Version 2.0 included additional Service software applications and COTS integrated with the COE including UB, APPLIX, JMCIS, CHATTER, GSORTS, LOGSAFE, FAPES, JFAST, UCCS, DART, IMS/RFM, S&M, and JDISS. The segments were tested following the methodology described in the previous paragraphs. Unit, component, and configuration item tests were done by the developing agency. Compliance, functional, installation and configuration definition tests were done by JIEO.

c. Version 2.1 included several new and updated segments to include the following: AIRFIELDS, AMHS, APPLIX, CCAPPS, Executive Manager, FRAS, FTP, COE, GSORTS, GTN, IMS_RFM, RDA, JMCIS, MEPES, JEPES, JOPES Core Database, Scheduling and Movement (S&M), RFA, EVAC, JOPES AHQ and TARGET. The complete list of segments included in GCCS 2.1 is documented in the GCCS 2.1 Version Description Document. A GCCS 2.1 multi-node SIPRNET test among the DISA/OSF, JITC and JDEF was completed in September, 1995 as was GCCS 2.1 JOPES developmental testing. The results of the functional testing of GCCS 2.1 and SIPRNET multi-node tests documented software deficiencies that were being corrected as part of 2.1 updates.

d. Version 2.2 included fixes to GSPRs, several updated segments, a patch roll up AMHS, CCAPS, DART, IMS_RFM, LOGSAFE, RDBMS, PERL, S&M, SYBASE and TCCESI, as well as the added features of VOLUME MANAGER, NETSCAPE BROWSER 3.0, MAIL SERVICES, and EMPIRE. The complete list of segments included in GCCS 2.2 is documented in the GCCS 2.2 Version Description Document. A GCCS 2.2 multi-node SIPRNET test among the DISA/OSF, JITC and CENTCOM was completed in January, 1997. The results of the functional testing of GCCS 2.2 and SIPRNET multi-node tests documented software deficiencies that are being corrected as part of 2.2 updates.

e. The software risk, maturity and other related issues will be addressed post-SOR. However, a history of the GSPRs will be available during MDT&E. The software risk management will follow the guidance provided in the following and other pertinent documents.

(1) Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS), Specification/Draft, Version 3.0, January 1, 1997. OPR: DISA Chief Engineer.

(2) Director, TSE&E, OUSD/A&T Memorandum, Subject: DTSE&E Policy Guidance for Software-Intensive Systems in Support of Recommendations from the GAO, 23 May 94.

(3) OUSD, Operational Test and Evaluation Memorandum, Subject: Software Maturity Criteria for Dedicated Operational Test and Evaluation of Software-Intensive Systems, 31 May 94.

3.3 Future Modified Developmental Test and Evaluation (MDT&E). MDT&E for GCCS version 3.0 and future versions will follow the testing outlined in the paragraphs above. Table III-3 lists the future test events. Future revisions of the TEMP will include follow-on test events.

Table III-3. GCCS Future Developmental Test & Evaluation Events

Software Version	Software Description	Evaluation Objective	Test Event(s)	Limitations
3.0	JOPES Unified Build Service Interface Tests (AFGCCS, AGCCS, MAGTFII) Automated message handling system Teleconferencing Joint mission applications Reference File Administration Other	Determine whether to field the version 3.0. Decisions will be based on the satisfaction of the J3 Entrance Criteria in Appendix G. Compliance with DII COE I&RTS	(1) Unit, Component, Configuration Item Tests. (2) Database synchronization (3) Database Backup/Recovery Test. (3) Database Snapshot (4) Multi-node User Test (MUT) (5) Stress Test Schedule TBD (6) Installation Test (7) Compliance Test	Crisis level test scenarios
3.X (Tentative)	Additional CINC/Service applications	Determine entry into OT&E Compliance with DII COE I&RTS	(1) Unit, Component, Configuration Item Tests. (2) Database synchronization (3) Database Backup/Recovery Test. (3) Database Snapshot (4) Multi-node User Test (MUT) (5) Stress Test Schedule TBD (6) Installation Test (7) Compliance Test	Crisis level test scenarios

PART IV

OPERATIONAL TEST AND EVALUATION OUTLINE

4.1 Operational Test and Evaluation (OT&E) Overview

a. Purpose. To determine the operational effectiveness and operational suitability of GCCS V3.0 in support of a Joint Staff J-3 decision concerning declaration of V3.0 as the DoD Command and Control System of Record.

b. Scope. The JITC, in collaboration with the Service Operational Test Activities, will conduct the OT under operationally realistic conditions using production representative equipment suites and actual operator personnel. Test activities will occur at operational sites and at laboratory sites. Two primary measures of effectiveness (MOEs) will be evaluated:

- Primary MOE 1. Success of Mission Tasks.
- Primary MOE 2. Success of Mission Support Tasks.

These MOEs are investigative; no criteria are established for number or percent of tasks successfully completed.

Figure 4-1 illustrates the OT&E concept. OT will consist of three phases and will be supported by data from DT. The three OT phases may overlap and are:

- **Mission Support Test.** This phase will occur at multiple sites. The focus will be to evaluate the success of Mission Support Tasks as performed by system administrators, data base administrators, system security administrators, and other support and administrative personnel.
- **Evaluation of training, documentation, and user support.** This phase does not include test activities. It includes evaluation only. It is designed primarily to determine the degree to which deficiencies previously observed in training, documentation, and user support (for example, help desk support) have been corrected. User support activities will be evaluated as they currently exist for GCCS Version 2.2. User training programs established for V3.0 at JTO and AETC will be evaluated. V3.0 user documentation will be evaluated.

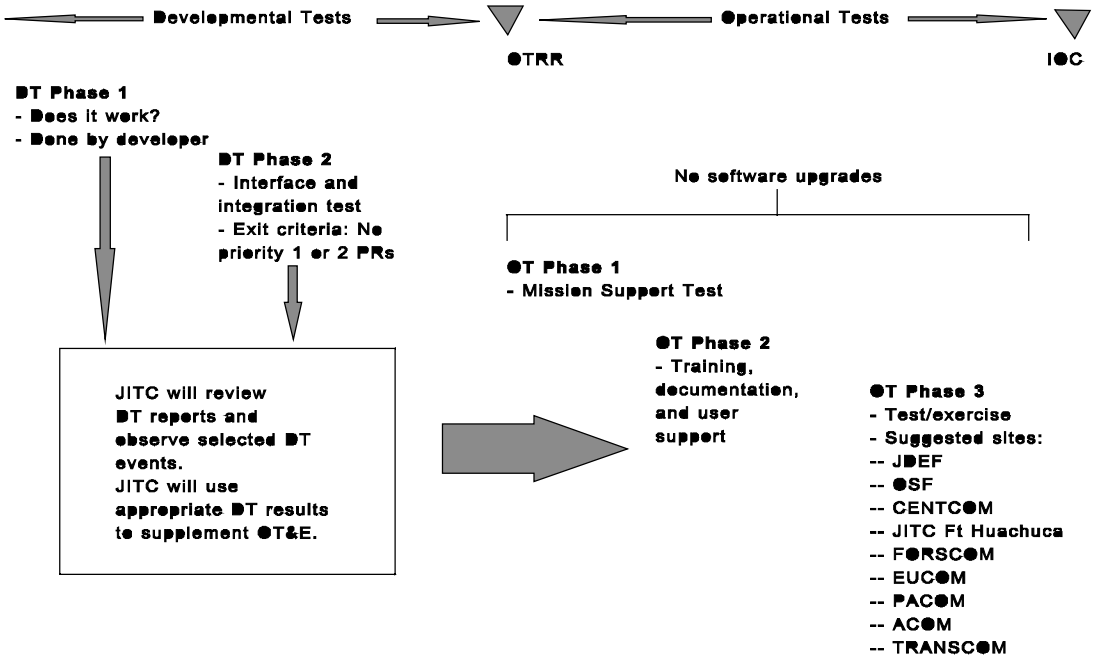

Figure IV-1. GCCS Version 3.0 OT&E Strategy

- **Simulated Crisis Situation.** The user community (Joint Staff and CINCs) will designate participating operational sites. The site designated as the supported CINC will select an OPLAN to use for test purposes. Actual users at operational sites will use GCCS to support crisis action planning and execution. It is important to select a robust plan that will exercise a broad representative sample of GCCS functions as identified in the RID (for example, JOPES, COP, intelligence, SORTS, and miscellaneous functions).

The system configuration will be established at the start of the installation test and will not be changed during this phase except as determined necessary by the JITC to support test operations. It may be necessary (and desirable) to make configuration changes after the installation test and before the TCPX. The GCCS PMO will coordinate with the JITC prior to making such changes. The system configuration will be re-established at the start of the TCPX and will not be changed during this phase except as determined necessary by the JITC to support test operations.

c. Joint Interoperability. The Joint Interoperability Test Command (JITC) is required by DODI 4630.8 and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01A to certify C4I systems for interoperability with Joint Systems with which they have a requirement to exchange information. At the end of Developmental Testing (DT), JITC must certify

conformance of standards and at the end of Operational Test and Evaluation (OT&E), JITC must certify interoperability. JITC will review GCCS test plans and procedures to ensure that the data to be collected meet the JITC requirements. JITC will monitor interoperability requirements during various GCCS tests and use the data to evaluate system interoperability.

The effective exchange of electronic and hardcopy information is critical to deliberate and crisis planning/execution. The success of GCCS planning is directly related to the information the planner has to use. This information is primarily obtained by electronic means. Similarly the successful execution of the plan is directly related to the information provided to the Warfighter.

4. 2 Critical Operational Issues.

System requirements for GCCS Version 3.0, as established in the Functional Description, lead to these five critical operational issues:

Operational effectiveness. Primary MOE 1, Success of Mission Tasks, is the principal test measure for operational effectiveness.

> **COI 1. Mission performance.** Does the GCCS support warfighters in accomplishing deliberate and crisis action planning and execution in an operational environment?
>
> This COI will be evaluated on the basis of Mission Task success in the context of an operationally realistic TCPX.
>
> **COI 2. Interoperability.** Does the GCCS support the effective exchange of information required to plan and execute missions? The areas that will be assessed to answer this COI are:
>
> 1. The interoperability of GCCS with other DoD systems.
>
> 2. The capability provided to the planner to use information provided by external organizations and to produce information used by external organizations.
>
> **COI 3. Security.** Does the GCCS architecture provide the necessary security precautions to protect the military operations and national objectives supported by the GCCS?

Operational suitability. Primary MOE 2, Success of Mission Support Tasks, is the principal test measure for operational suitability.

> **COI 4. Mission Support.** Can GCCS be installed, configured, and maintained effectively at operational sites? This COI will be evaluated on the basis of Mission Support Task success in the context of the Mission Support Test.

COI 5. Supportability. Is the GCCS capable of supporting sustained operations in an operational environment?

a. User support. Is the GCCS help desk and supporting infrastructure capable of supporting GCCS users in an operational environment?

b. Training. Does the training program provide GCCS users (system and database administrators, functional users, etc.) the skills required to perform their operational tasks on the GCCS?

c. Documentation. Does the user-level documentation provide GCCS users adequate and complete information on how to accomplish their operational tasks on the GCCS?

d. Reliability, availability, and maintainability (RAM). Does GCCS V3.0 possess RAM characteristics equal to or greater than previous versions?

4.3 Operational Test and Evaluation to Date

No OT&E has been performed for GCCS Version3.0. However, the JITC, Service OTAs, and several user groups conducted OT&E of V2.1 during April-August 1996. As a result, the Joint Staff declared V2.1 the DoD C2 System of Record and shut down the legacy World Wide Military Command and Control System (WWMCCS). The JITC, CENTCOM, and COMOPTEVFOR conducted an operational assessment of V2.2 in December 1996. As a result, V 2.2 was distributed to the field as a replacement for V2.1.

It is currently planned that V3.0 will add some new functionality over that in V2.2. The primary objectives of V3.0 are:

- replace the GCCS COE with the DII COE
- upgrade versions of the GCCS workstation operating systems
- upgrade the version of the Oracle Relational Database Management System (RDBMS)
- replace the current government-developed desktop with a commercial desktop.
- Provide some high priority GSPR fixes
- provide some new functionality in the areas of:
  JAVA based Airfields
  Tactical METOC capability
  JTAV client
  JPAV client
  TBMD Segment
  MIG/MIGDB access and display (Renamed to TC4I)
  Imagery Product Library (IPL) access and display
  TRE interface to support TBMD
  Production quality receive-only interfaces for:
  TIBS, TADIL B, PLRS/EPLRS

Thus it is necessary to test the existing and new functionality in the context of the new COE, operating system, RDBMS, and desktop.

Testing of V3.0 is further required because OT of V2.1 and 2.2 was limited by these factors:

- **Questionnaire responses of limited value in assessing GCCS V2.1.** In testing V2.1, 28 of 48 test measures were based on user assessments; the primary data source for these assessments was intended to be user questionnaires. However, because of limitations in the collection of questionnaire responses, the JITC assigned a low weight to the responses and instead relied on other sources for the user assessments.

- **Functional checkout of GCCS V2.2 not operationally realistic.** The OA of V2.2 was based on Beta testing, which consisted primarily of functionality checks performed without a realistic operational scenario.

4.4 Future Operational Test and Evaluation.

Testing of V3.0 will overcome the shortcomings noted above for testing of V2.1 and V2.2.

4.4.1 DT Support of OT.

The JITC will review DT test results, which will be provided by the PMO, and may observe selected DT events. JITC will use applicable DT results to support the OT&E. The JITC will be leading the DT Stage III and beta testing as a part of OT Readiness Review.

4.4.2 Mission Support test.

The test will be task driven, and the evaluation will focus on success of Mission Support Tasks accomplished by test players.

a. Measuring Mission Support Task Success

A list of potential Mission Support Tasks is at PART IV Appendix, Table 9. The user community will determine the final task list. A Mission Support Task is an action that must be performed by a GCCS system administrator, database administrator, security manager, or other support person to install, set-up, configure, or otherwise prepare the system for operational use; it should take about one to four hours to complete.

The user community will establish the criterion for success of each task based on timeliness, ease of performance and adequacy of training and documentation to perform the task. The following is a proposed scale:

Unsuccessful. The task could not be performed by the assigned personnel.

Marginally successful. Task performed with workarounds. Documentation lacks sufficient details. Task not fully covered in applicable training.

Fully successful. Task easily performed in a timely manner. Task fully covered in applicable training. Documentation accurate, complete, and readily available.

Highly successful. Task performance exceeds requirements. Task training and documentation exceed requirements.

The user community may categorize the tasks according to their importance to overall mission accomplishment. Is so, the JITC will consider the user priorities in the evaluation.

The user community will provide subject matter experts (SMEs) to evaluate success of Mission Support Tasks accomplished by test players. The JITC will investigate causality for any non-successful Mission Support Tasks.

b. Test sites. Test sites will include operational sites and lab sites. To preclude disruption of operational missions, operational sites will use spare (not operational) equipment suites.

4.4.3 Evaluation of training, documentation, and user support**.**

This phase of OT focuses on COI 5 Supportability (except RAM). It may be completed before the other two OT phases. It will consist of three separate evaluations, as described below.

Training evaluation. JITC will evaluate the following training courses conducted by the JTO and AETC:

Training to support Mission Support Tasks
- Database administrator training
- System administrator training (HP/UX, Solaris, NT)
- Security manager training
- Network manager training
- AMHS administrator training

Training to support Mission Tasks
- GCCS User Introduction
- GCCS Action and Planning Staff Orientation
- Training to support user requirements for:
  - Resource and unit monitoring (GSORTS and RFA)
  - Conventional Planning and Execution (JOPES and JOPES-related)
  - Other Joint requirements (Airfields, EVAC, teleconferencing applications, TELNET and file transfer)
  - Interoperability (AMHS)

  - Common Operational Picture

Air Tasking Order
Access to intelligence data
Support applications such as Applix

The evaluation will focus on the effectiveness of the training to prepare the user to perform the mission using GCCS V3.0. A principal input to the evaluation will be interviews with personnel at selected sites to determine the user's perspective of training effectiveness. The JITC will attend selected courses to support the evaluation of training.

Documentation evaluation. This evaluation will commence as documentation becomes available for review in draft form. The intent is to influence final documentation. JITC will review and evaluate the following user documentation:

Operator's manual
Installation procedures
System administrator's manual
Software user's manual
Other user documentation such as application-specific user manuals .

In addition, JITC will interview personnel at selected sites. The evaluation will focus on the following factors:

Availability of documentation to users at operational sites, to include ease of access, downloading, printing, and declassification.
Accuracy
Usefulness
Currentness with respect to V3.0 software
Completeness.

User support evaluation. JITC will review and evaluate existing procedures for user support; that is, the procedures in place for V2.2. This evaluation applies to V3.0 because the user support concept does not change between V2.2 and V3.0. This will include (but will not be limited to) the Help Desk. This review will include interviews with personnel at selected operational sites. The evaluation will focus on:

Effectiveness of user support in providing technical assistance to the user
Accuracy of responses
Timeliness of responses
Completeness of responses
Usefulness of responses to the user in supporting the user mission.

4.4.4 Simulated Crisis Situation.

The exercise will include a planning phase and an execution phase. Staff elements from the supported and supporting CINCs, appropriate components, a simulated JTF, and the NCA will participate. The test will be task driven, and the evaluation will focus on success of Mission Tasks accomplished by test players.

a. Measuring Mission Task Success. Figure IV-2 illustrates the concept for evaluation of Mission Task Success. The following discussion amplifies the concept.

A list of potential Mission Tasks is at PART IV Appendix, Tables 2 through 8. The user community will determine the final task list. A Mission Task is a staff action that requires GCCS support to accomplish and that has a defined product; it should take about one to four hours to complete.

The user community will establish the criterion for success of each task based on the timeliness, accuracy, completeness, and usefulness of the task product. The following is a proposed scale:

> Unsuccessful. No product or product cannot be used by the intended recipient for the intended purpose.
>
> Marginally successful. Product requires workarounds to produce, or the intended recipient must use workarounds to use the product for mission accomplishment.
>
> Fully successful. Product is sufficiently timely, accurate, complete, and useful that it fully supports mission accomplishment by the intended recipient.
> Highly successful. Product exceeds requirements for timeliness, accuracy, completeness, or usefulness.

The user community may categorize the tasks according to their importance to overall mission accomplishment. If so, JITC will consider the user priorities in the evaluation.

The user community will provide subject matter experts (SMEs) to evaluate success of mission tasks accomplished by test players. The JITC will investigate causality for any non-successful Mission Tasks.

b. Test sites. Test sites will include operational sites and lab sites. To preclude disruption of operational missions, operational sites will use spare (not operational) equipment suites, as available. Potential sites include: NMCC, CENTCOM, ACOM, EUCOM, TRANSCOM, OSF, JITC Ft Huachuca lab, and JDEF. The sites will be configured to represent the NCA, supported CINC and components, supporting CINCs, JTF and components, and other players as necessary.

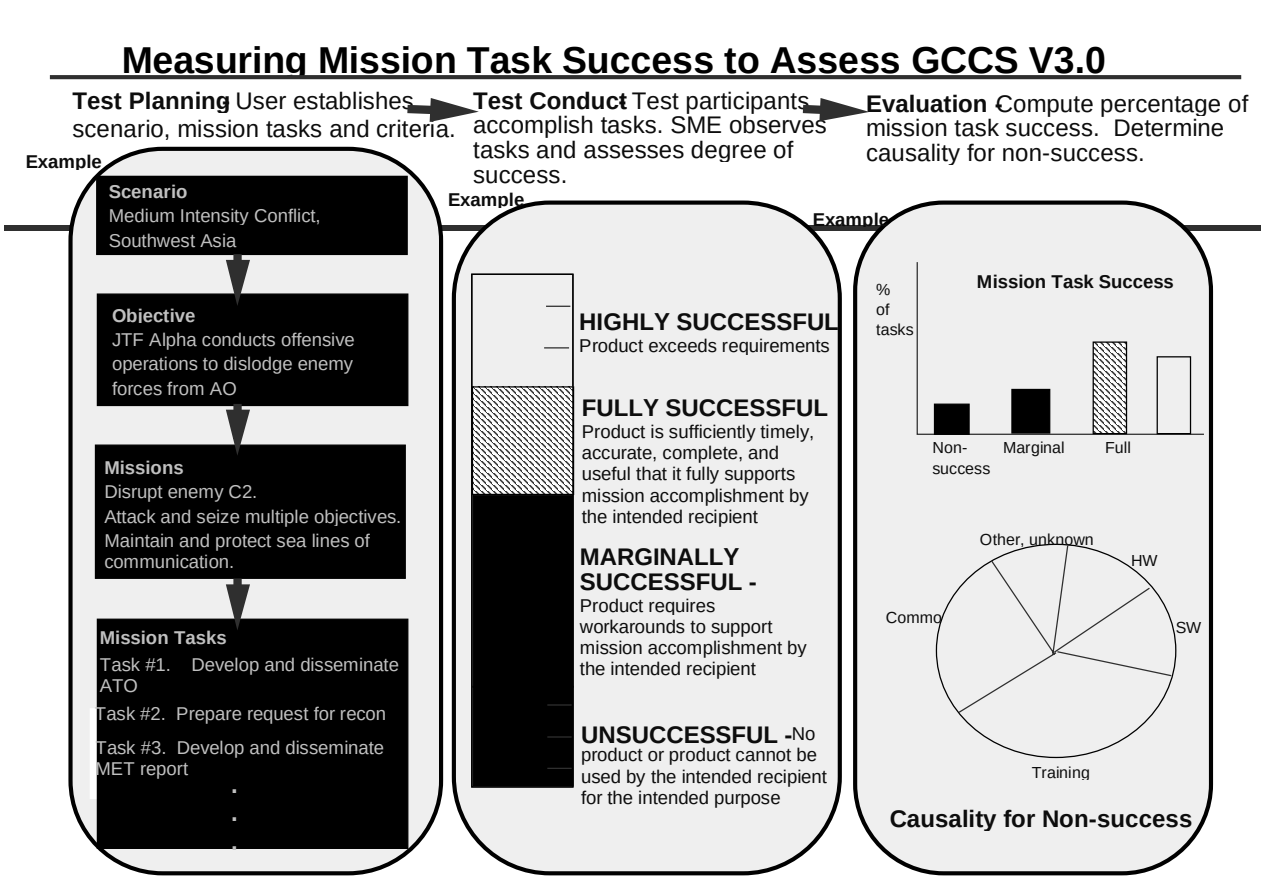

Figure IV-2. Measuring Mission Task Success

PART IV APPENDIX **- MISSION TASKS AND MISSION SUPPORT TASKS**

The following information has been extracted from the GCCS User Characterization Profile and other sources to produce a partial listing of possible mission/mission support tasks for testing GCCS Version 3.0.

Crisis Action Procedures. CAP provides a framework for describing the unfolding of a crisis requiring a military response. Table 1 lists the six CAP phases.

Table 1. CAP Phases

Phase	Title
I	Situation Development
II	Crisis Assessment
III	Course of Action Development
IV	Course of Action Selection
V	Execution Planning
VI	Execution
VII	Redeployment

Each phase is punctuated by one or more scenario events. The scenario event usually triggers a response from one or more of the Joint Planning and Execution Community (JPEC) players in the crisis. Many responses consist of an activity supported by the GCCS. The trace from a scenario event to the GCCS activity performed by specific JPEC member(s) is contained in the CAP Matrix that follows.

Participant. The scenario event triggers a response/action at certain levels in the JPEC. The actions contained in the matrix are limited to those participants with the most GCCS play. The participants listed in the matrix are:

CJCS - Chairman of the Joint Chiefs of Staff
SPD - Supported Commander
SPG - Supporting Commander
USTC - United States Transportation Command
SVC - Services

Tasking arrangement. Tables 2 through 7 contain the mission tasks for each respective phase. Table 8 contains additional mission tasks which were not specified in the GCCS User Characterization Profile, but each user should integrate these tasks into table 2 through 7 where most appropriate for their activity. In addition, each user should test desktop functions and other supporting applications within appropriate mission task areas.

Table 9 contains other Mission Support Tasks for Systems Administrators, Security Administrators, Database Administrators, Functional Database Managers, and Track Database Managers.

Table 2. Mission Tasks, Crisis Action Planning Matrix, Phase I

Phase I - Situation Development Phase I begins with an event having possible national security implications and ends when the CINC submits his assessment of the situation to the National Command Authority (NCA) and the Chairman of the Joint Chiefs of Staff.				
PARTICIPANT	**BACKGROUND ACTION**	**MISSION TASK**	**OUTPUT/PRODUCT**	**ANTICIPATED APPLICATIONS**
CJCS	Monitor the situation and evaluate reports from all sources; Request an assessment report from the supported commander	Generate a GENSER message to SPD	Message to SPD	AMHS
SPD	Review message	Provide a CINC's assessment report	OPREP-3 message	AMHS

Table 3. Mission Tasks, Crisis Action Planning Matrix, Phase II

Phase II - Crisis Assessment
Phase II begins with a report from the supported commander and ends with a decision by the NCA to return to the pre-crisis situation, or to have military options developed for possible consideration and possible use.

PARTICIPANT	BACKGROUND ACTION	MISSION TASK	OUTPUT/PRODUCT	ANTICIPATED APPLICATIONS
ALL	Anticipation of action	Review OPLANs and CONPLANs for applicability	List of available/applicable plans	RDA AHQ
ALL	Anticipation of action	Review force readiness	Unit readiness reports	GSORTS AHQ
CJCS	Request SPD take action	Request SPD establish a crisis Newsgroups	Message to SPD	AMHS
SPD	Respond to message	Implement the crisis Newsgroups	Newsgroups established; message to participants to join	Newsgroups AMHS
ALL	Respond to message	Subscribe to Newsgroups	Newsgroups actions	Newsgroups
CJCS	Require USTC review strategic lift asset employment availability	Generate a Newsgroups message to USTC	Newsgroups message	Newsgroups
USTC	Review the status of strategic lift assets	Review lift asset availability; Review lift asset status	Lift Asset Reports	GSORTS
USTC & SPD	Determine amount of lift available for operation	Publish numbers of lift assets to be made available	Updated transportation Models	Newsgroups ADANS STRADS SEASTRADS

Table 4. Mission Tasks, Crisis Action Planning Matrix, Phase III

Phase III - Course of Action Development
Phase III begins with a decision to develop possible military Courses of Action (COAs), normally transmitted by a CJCS Warning Order, and ends when COAs are presented to the NCA.

PARTICIPANT	BACKGROUND ACTION	MISSION TASK	OUTPUT/PRODUCT	ANTICIPATED APPLICATIONS
CJCS	Establish command relationships; State mission, objectives, and known constraints; Direct the development of COAs	Publish Warning Order	Warning Order message published	Newsgroups AMHS
ALL except CJCS	Respond to Warning Order; Initiate development of possible COAs using GCCS	Review existing OPLANs/ TPFDDs	Existing files access	RDA AHQ GSORTS
ALL	Update an existing OPLAN	Refine existing supported/supporting OPLANs/TPFDDs	Modified OPLAN/TPFDD	RDA AHQ GSORTS
SPD	Initiate development of new COAs /TPFDDs	Develop new COAs/TPFDDs using GCCS	Newly initiated plan	SS RDA
ALL except SPD and CJCS	Receive new TPFDD	Review and modify new TPFDD	Updated new TPFDD	RDA AHQ PDR GSORTS IMS DART

Table 4. Mission Tasks, Crisis Action Planning Matrix, Phase III (continued)

PARTICIPANT	BACKGROUND ACTION	MISSION TASK	OUTPUT/PRODUCT	ANTICIPATED APPLICATIONS
SPD	Prepare new TPFDD for evaluation	Generate sustainment records for the new TPFDD using JEPES	TPFDD file processing	IMS JEPES LOGSAFE
		Generate sustainment records for the new TPFDD using MEPES	TPFDD file processing	IMS MEPES LOGSAFE
		Generate sustainment records for the new TPFDD using LOGSAFE	TPFDD file processing	IMS LOGSAFE
SPD	Request evaluation of proposed COAs	Publish an Evaluation Request; Evaluate availability, combat readiness and suitability of forces; Evaluate availability of sustainment; Evaluate database completeness	Newsgroups Evaluation Request	Newsgroups
ALL except SPD and CJCS	Receive and review Evaluation Request	Perform an evaluation of the COAs/TPFDDs	Logical Errors Report; TCC Pre-edit Report	RDA AHQ PDR
SPD	Fatal Error Free TPFDD required for transportation analysis	Produce a Fatal Error Free TPFDD	Logical Errors Report; TCC Pre-edit Report TPFDD ready for transportation analysis	Newsgroups RDA
SPD	Request Deployment Estimate by USTC	Request USTC develop a preliminary Deployment Estimate	Newsgroups request for Deployment Estimate	Newsgroups

Table 4. Mission Tasks, Crisis Action Planning Matrix, Phase III (continued)

PARTICIPANT	BACKGROUND ACTION	MISSION TASK	OUTPUT/PRODUCT	ANTICIPATED APPLICATIONS
USTC	Review the request for a Deployment Estimate	USTC conduct Deployment estimates on each viable COA/TPFDD	Land summary and associated graphs and reports; Sea summary and associated graphs and reports; Air summary and associated graphs and reports; Airlift summary profile; Sealift summary profile; Lateness by supply class reports; Force Module Closure Profiles	IMS JFAST
		Prepare and submit Deployment Estimate Response message	Deployment Estimate Response message	Newsgroups
SPG	Preparation and submission of Evaluation Response to the SPD; Review of Deployment Estimate Response	Prepare an Evaluation Response message (OPREP-1)	Evaluation Response message	Newsgroups
SPD	Preparation and submission of Commander's Estimate; Recommendation of a COA; Review of Evaluation Response	Prepare and submit the Commander's Estimate	Commander's Estimate	Newsgroups
ALL	Review of Commander's Estimate			

Table 5. Mission Tasks, Crisis Action Planning Matrix, Phase IV

Phase IV - Course of Action Selection
Phase IV begins when COAs are presented to the NCA and ends when a COA is selected. The primary activity in this phase of crisis planning rests with the Chairman of the Joint Chiefs of Staff and NCA. All other members of the JPEC continue their activities as described in Phases II and III.

PARTICIPANT	BACKGROUND ACTION	MISSION TASK	OUTPUT/PRODUCT	ANTICIPATED APPLICATIONS
CJCS	Review and Evaluate COAs presented in the Commander's Estimate; Alert Order is published directing execution planning activities commence for Selected COA	Alert Order published directing execution planning activities commence for Selected COA	Alert Order	Newsgroups AMHS
ALL	Receive and review Alert Order			Newsgroups
SPD	Publish a TPFDD Letter of Instruction (LOI)	Publish a TPFDD LOI that provides procedures for the deployment, replacement, and redeployment of the forces in support of Selected COA	TPFDD LOI	Netscape Newsgroups

Table 6. Mission Tasks, Crisis Action Planning Matrix, Phase V

Phase V - Execution Planning
Phase V begins when a Planning or an Alert Order is received and ends when an executable OPORD is developed and approved for execution on order. Based on receipt of the Alert Order, activities commence for further selected COA refinement and preliminary scheduling activities.

PARTICIPANT	BACKGROUND ACTION	MISSION TASK	OUTPUT/PRODUCT	ANTICIPATED APPLICATIONS
NOTE: The following incremental cycle includes: validation of movement requirements, scheduling of organic and strategic lift, the allocation of requirements to carriers, the reporting of actual carrier movements, and the manifesting of requirements to carriers. Any carrier itinerary changes or diversions will continue until the deployment is complete or the crisis subsides (combined Phases V and VI).				
SPD SPG USTC	Review the TPFDD LOI	Confirm and adjust selected COA force requirements/sustainment requirements and priorities	Adjusted TPFDD	RDA AHQ
SPG SPD	TPFDD adjusted to LOI	Schedule/allocate organic movements for the first increment of deployment	Scheduled TPFDD	S&M
SPG	TPFDD scheduled	Identify force and sustainment shortfalls	Shortfalls listings	RDA AHQ Newsgroups
SPD	Review SPG force and sustainment shortfall messages	Validate the first deployment increment (first 7 days of airlift and first 30 days of sealift)	Transportation Pre-edit Report; Validated first deployment increment	RDA PDR
SPD	Validated first deployment increment	Notify the JPEC when the first deployment increment is validated	Validation message	Newsgroups TCCESI

Table 6. Mission Tasks, Crisis Action Planning Matrix, Phase V (continued)

PARTICIPANT	BACKGROUND ACTION	MISSION TASK	OUTPUT/PRODUCT	ANTICIPATED APPLICATIONS
ALL	Receive and review Validation message			Newsgroups
USTC (AMC)	Validated increments will be scheduled	Develop and enter Common-User Air Movement Schedules (7 days)	7 days of air schedules	S&M GTN ADANS TCCESI
USTC (MTMC) (MSC)	Validated increments will be scheduled	Develop and enter Common-User Surface Lift schedules (30 days)	30 days of surface schedules	S&M GTN TCCESI
SPG	Validated increments will be scheduled	Develop and enter organic carrier schedules	Schedules for non-strategic lift legs	S&M
SPD	The SPD converts the COA into an OPORD	Convert the COA and publish an OPORD	Newsgroups OPORD	Newsgroups
ALL	Receive and review OPORD			Newsgroups

Table 7. Mission Tasks, Crisis Action Planning Matrix, Phase VI

Phase VI - Execution Phase VI begins with the decision to execute an Operation Order (OPORD), normally transmitted by a CJCS Execute Order, and continues until the crisis is resolved satisfactorily.				
PARTICIPANT	**BACKGROUND ACTION**	**MISSION TASK**	**OUTPUT/PRODUCT**	**ANTICIPATED APPLICATIONS**
CJCS	An Execute Order is published and issued directing the supported commander to execute his OPORD; The order directs the deployment/ employment of forces in selected COA	Issue Execute Order	Execute Order	Newsgroups AMHS
ALL	Direct mobilization activities; Coordinate with personnel centers and logistic agencies; Identify and confirm sustainment requisitions	Monitor the initial deployment of forces; Review deployment status of ULNs, UICs and Force Modules	Execution of movement	Newsgroups AHQ RDA S&M PDR
USTC (AMC)		Report Strategic Airlift Arrival and Departures for the first increment of movement (first 7 days)	Airlift movement	S&M
USTC (MTMC) (MSC)		Report Common-User Surface Lift Arrival and Departures for the first increment of movement (first 30 days)	Surface movement	S&M GTN
SPG	Actual arrivals/departures will be reported	Report arrivals and departures of non-strategic carriers	Non-strategic carrier movement reports	S&M
NOTE: The above incremental cycle includes: validation of movement requirements, scheduling of organic and strategic lift, the allocation of requirements to carriers, the reporting of actual carrier movements, and the manifesting of requirements to carriers. Any carrier itinerary changes or diversions will continue until the deployment is complete or the crisis subsides (combined Phases V and VI).				
SPD	JTF Deploys forward	Deploy GCCS forward	All required GCCS functionality usable in an austere comms environment	ALL

Table 8. Additional Mission Tasks

The following mission tasks are not included in the GCCS User Characterization Profile. They need to be inserted into the testing at appropriate places.

PARTICIPANT	BACKGROUND ACTION	MISSION TASK	OUTPUT/PRODUCT	ANTICIPATED APPLICATIONS
EVAC User	Non-combatant personnel need to be evacuated from area of interest (AOI)	Produce and print an evacuation list for country and district of AOI	EVAC report	EVAC
		Produce and print Evacuation Summary for country of AOI	EVAC summary report	EVAC
FRAS User	Fuel requirements must be programmed into planning	Produce and print a fuel resources report	Two FRAS files to process on PC FRAS	FRAS extract PC FRAS
Air Field Planner	Usable airfields must be made known to movement planners	Produce Airfields report for AOI	Airfields report	Airfields
Common Operational Picture Users	Maps for AOI may be viewed as desired, with available tracks for all reported activity	Bring up Common Operational Picture (COP) without filters set	Display of map and tracks (may be very cluttered, depending on amount of message traffic)	COP
		Filter out undesired tracks	Less cluttered display	COP
	Users without COP processing can view a snapshot of COP by using ELVIS (in receive only mode)	This task will require co-located COP and non-COP workstations; Visually verify that the ELVIS picture matches the COP Picture	Active COP picture and ELVIS snapshot agree	COP ELVIS
TARGET users	Additional tools available	Exercise the TARGET functionality		TARGET MATT

Table 8. Additional Mission Tasks (continued)

PARTICIPANT	BACKGROUND ACTION	MISSION TASK	OUTPUT/PRODUCT	ANTICIPATED APPLICATIONS
UB	Air Tasking Orders can be reviewed, segmented, and segments transmitted to components as needed	Receive an ATO	ATO message	UB
		Segment the ATO	Segments of ATO	UB
		Transmit the ATO segments to the components they apply to	Transmitted segments received by components	UB
COP Users	Execution of ATO results in air tracks being reported which will then appear in COP	Verify that during ATO execution, the reported air tracks correlate to the aircraft designated in the ATO	Air tracks in COP match ATO plans	COP
Intelligence System Users	Intelligence mission requires access to resources	Provide an intelligence resources report	Resources report	GRIS
		Produce a request for intelligence support	Intelligence support request	COLISEUM
JDISS Users		Execute the intelligence mission	Intelligence gathering of imagery and sensor data	JDISS
SVC	Service feeder systems must support GCCS with the new operating systems, new DII COE and new Oracle Relational Database Manager	Each service verify that the interfaces still work correctly	Services Interface Files	COMPASS COMPES MAGTF II RUDRS AMHS Newsgroups IRC

Table 8. Additional Mission Tasks (continued)

PARTICIPANT	BACKGROUND ACTION	MISSION TASK	OUTPUT/PRODUCT	ANTICIPATED APPLICATIONS
SVC/remote users	Access to documentation must be verified	Access GCCS homepage and view/ download new documents	Documents on line	Netscape Browser
SVC	Maintenance of and access to Status of Resources and Training (SORTS) must be verified	Each service use access through GSORTS to verify that the service updates to SORTS is being processed and passed to GSORTS and GCCS users	GSORTS listing of selected service units	GSORTS SORTS

Mission Support Tasks. The following table presents examples of Mission Support Tasks. These tasks are primarily for Systems Administrators, Security Administrators, Database Administrators, Functional Database Managers, and Track Database Managers.

Table 9. Mission Support Tasks

PARTICIPANT	BACKGROUND ACTION	MISSION SUPPORT TASK	OUTPUT/PRODUCT	ANTICIPATED APPLICATIONS
System Administrator (SA)	SA is responsible for installing GCCS applications on local site	Determine local site configuration unique settings	List of unique settings, equipment, and application install requirements	Pre-planning
		De-install segments to be replaced	Cleaned out disk space	Command line or INSTALLER
		Install new Solaris	New operating system	INSTALLER
		Install new Desktop/EM server	New EM Server	INSTALLER
		Install new RDBMS (ORACLE)	New RDBMS	INSTALLER
	Establish/update the domain name service	Install the local domain name server	Local DNS Server	INSTALLER
		Update DNS as needed	Updated DNS	DNS Admin
	Establish/update the NIS+ service	Install the local NIS+Server	Local NIS+ Server	Command line, Solaris
		Create NIS+ replicas		Command line, Solaris
		Update NIS+ as needed	Updated NIS+	NIS+ Admin
	Install new segments in proper order	Install new segments in proper order	New segments on system	INSTALLER
	Provide printer support to users	Configure and manage printers for user access	Current printer file printer table	PRINTER Admin

Table 9. Mission Support Tasks (continued)

PARTICIPANT	BACKGROUND ACTION	MISSION SUPPORT TASK	OUTPUT/PRODUCT	ANTICIPATED APPLICATIONS
SA (continued)	Users require accounts and permissions to access applications	Provide accounts for database user	DBUSER tables	DBUSER
		Provide user accounts for general access	User account groups	EM
	Users require accounts and permissions to access applications	Set permissions	User permissions	EM
	Software licenses must be available and administered to provide user access to applicable applications	Acquire licenses as required; Provide user access	Usable licensed applications	License Admin
	Provide for configuration management	Apply file and directory listings of all applications	File system management	Command line
	Provide Apply user support	Process Inter-relationship specifications	System Trouble shooting	Command line
	Teleconferencing capabilities must be provided to users	Install teleconferencing applications	Teleconference capabilities	IRC Newsgroups World Wide Web
	Provide mail service	Install mail service	Sendmail application	Command line Solaris
		Maintain mail admin files	Usable mail system	Sendmail
	Provide problem corrections	Halt system operations	All processing stops	
		Reboot system in single user mode	Only root user (SA) can access system	
		Reboot system in normal mode	All authorized users may log in and process applications	

Table 9. Mission Support Tasks (continued)

PARTICIPANT	BACKGROUND ACTION	MISSION SUPPORT TASK	OUTPUT/PRODUCT	ANTICIPATED APPLICATIONS
SA (continued)	Provide system backup and recovery services	Perform routine scheduled backups	Backup files on tape or disc	Backup procedures
		When needed, perform system recovery actions	Recovered system; ready to resume processing	Recovery procedures
	Provide GSORTS administration	Provide for GSORTS updated information	Up-to-date GSORTS files	
SA and/or Sec Mgr	Provide security aspects of mission support	Setup and maintain user access accounts	User accounts files	
		Setup and maintain system and user profiles	Profile tables	
		Maintain roles in account groups	Account group roles	
		Provide system audit capabilities	Audit logs	
		Provide password administration	Password controls	
DataBase Administrators (DBA)	Provide reliable database support to authorized users	Establish and maintain authorized database structure	Prescribed databases	Oracle Tools
		Perform database backup	Backup data on storage media	Oracle Tools
		Provide database recovery	Reload data from backup and process files	Oracle Tools
	Provide database maintenance capability	Apply Entity Relationship Model/ Diagram and Data Dictionary	Database Management	Command line

Table 9. Mission Support Tasks (continued)

PARTICIPANT	BACKGROUND ACTION	MISSION SUPPORT TASK	OUTPUT/PRODUCT	ANTICIPATED APPLICATIONS
DBA (continued)	Provide for alternate database access	Provide for user access and permissions at alternate database sites	User access and permissions files at alternate database site	Oracle Tools
		Provide alternate database access when needed	Remote database access to alternate site	
JOPES Functional Database Manager (FDBM) or Track Database Manager (TDBM) as appropriate	Use the JOPES FDBM or TDBM responsibilities listing as a guide to test and evaluate mission support functions in the following areas:			
	Administrative	Permissions management		
		Teleconferencing (Newsgroups)		
		Installations		
		Backup/Recovery (JOPES Database)		
		Backup/recovery Individual TPFDDs		
		Continuity of Operations Plan (COOP)		
		Admin reporting (management)		
	OPLAN Management	OPLAN initialization		
		OPLAN type/distribution/access		
		OPLAN status		
		OPLAN offload/reload		

Table 9. Mission Support Tasks (continued)

PARTICIPANT	BACKGROUND ACTION	MISSION SUPPORT TASK	OUTPUT/PRODUCT	ANTICIPATED APPLICATIONS
FDBM or TDBM (continued)		OPLAN deletes		
		Set C-Day/L-Hour		
		Reset C-Day/TCC indicators		
		OPLAN synchronization		
		Reporting (user)		
	Network management/monitoring	Site status		
		Transaction processing/flow (local)		
		Database maintenance and statistics		
		Transaction processing/flow (distributed network)		
		Reporting (transactions)		
	Provide JMCIS administration	Provide for JMCIS channels and JMCIS feeds	Up-to-date JMCIS files	

PART V

TEST AND EVALUATION RESOURCE SUMMARY

5.1 Test and Evaluation Resource Summary.

a. Test Articles. GCCS test articles include all software and hardware configurations required to support GCCS Versions 3.0. Also included are software and hardware configurations of Joint/CINC/Service systems that are to interoperate with GCCS.

b. Test Sites and Instrumentation. The user community, ICW Joint Staff J-3 and the Program Management Office will select operational sites to serve as test sites. Each site will be configured in an operationally realistic manner.

c. Test Support Equipment. Hardware (e.g., personal computers) and software (e.g., data base software) are required to support any data reduction and test reporting requirements. Test support equipment at the three test sites mentioned above include five complete starter set configurations each with one database server, two application servers and two clients. Additionally, each site includes a communications router which provides access to the secret network. Each test system will be installed with the GCCS release and all required COTS software components to include operating system, Relational Data Base Management System (RDBMS) and network management software.

d. Threat Systems/Simulators. None required.

e. Test Targets and Expendables. None required.

f. Operational Force Test Support. A command post exercise (CPX) designed to assess crisis action and redeployment planning/execution on GCCS 3.0 functionality is planned during the user assessment. A letter of instruction describes the CPX along with exercise participants.

g. Simulations, Models and Testbeds. Terminal emulators are required to simulate multiple users on GCCS. The various Joint/CINC/Service interfaces will be stress loaded to test GCCS' operational effectiveness.

h. Special Requirements. None.

i. Test and Evaluation Funding Requirements. Program element 150K includes an estimated 1.5 million dollars for GCCS test and evaluation in each fiscal year.

j. Manpower Personnel Training. Training to support GCCS test and evaluation includes installation training designed to train personnel to install segments and load the database prior to the beginning of the user pre-assessment. The Joint Training Office (JTO) will provide training on the GCCS system administration and applications prior to the user assessment. Studies within each of the Services are currently underway to determine training requirements. Table V-2 lists

test personnel requirements for the OE.

Table V-2. Operational Test (OT) Personnel Requirements

EVENT	TEST PERSONNEL
Normal Operations	No dedicated personnel required. Users perform day-to-day task at 37 GCCS sites.
DT Phase 1 (User Involvement)	JITC/Users evaluation team: Sites, dates and numbers TDB.
DT Phase 3 (BETA Test)	JITC/Users evaluation team: Dates and numbers TDB.
Database Synchronization	Selected CINC/component sites: System Administrator, users. JITC: TDB data collectors OSF: TDB System Administrator, data collectors
JOPES Database Refinement Conference	JCS/J7 Test Team: (TBD) Users: Conference attendees JITC: TBD observers Components: Test personnel as coordinated
Operational (End-to-end) Test	Selected CINC/component sites: System Administrator, users, crisis action teams per J33 LOI.* JITC: TDB data collectors OSF: TDB System Administrator, data collectors

* Will be coordinated with J3

APPENDIX A

ACRONYM LIST

Ao	Operational Availability
ASD	Assistant Secretary of Defense
C2	Command and Control
C3	Command, Control, and Communications
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
C4IFTW	C4I For the Warrior
CCE	Continuous Comprehensive Evaluation
CINC	Commander In Chief
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
COA	Course of Action
COE	Common Operating Environment
CONOPS	Concept of Operations
COTS	Commercial Off-the-shelf
CPX	Command Post Exercise
CSCI	Computer Software Configuration Item
DDA	Designated Development Agency
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	Department of Defense
DODIIS	DoD Intelligence Information System
DOT&E	Director, Operational Test and Evaluation
DTE	Developmental Test and Evaluation
EPIP	Evolutionary Phased Implementation Plan
FCA	Functional Configuration Audit
FQT	Formal Qualification Testing
GCCS	Global Command and Control System
GOTS	Government Off-the-shelf
HEMP	High Altitude Electromagnetic Pulse
IOC	Initial Operational Capability
JCS	Joint Chiefs of Staff
JDEF	Joint Demonstration and Evaluation Facility
JIEO	Joint Interoperability Engineering Organization
JITC	Joint Interoperability Test Command
JMAS	Joint Mission Application Software
JOPES	Joint Operations Planning and Execution System
JSCP	Joint Strategic Capabilities Plan
JTF	Joint Task Force
JTO	Joint Training Office
LAN	Local Area Network
MCOTEA	Marine Corps Operational Test & Evaluation Activity

METOC	Meteorology and Oceanographic
MNS	Mission Needs Statement
MAOPR	Minimum Acceptable Operational Performance Requirement
MUT	Multi-node User Test
NBC	Nuclear Biological and Chemical
NCA	National Command Authority
O&M	Operations and Maintenance
OE	Operational Evaluation
OEC	Operational Evaluation Command
OPLAN	Operations Plan
OPTEC	Operation, Test, and Evaluation Command
OPTEVFOR	Operational Test and Evaluation Force
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
OSF	Operational Support Facility
OT&E	Operational Test and Evaluation
OTRR	Operational Test Readiness Review
PCA	Physical Configuration Audit
PM	Program Manager
PMO	Program Management Office
RDBMS	Relation Data Base Management System
RID	Requirements Implementation Document
SOR	System of Record
STT	Software Technical Test
T&E	Test and Evaluation
TAFIM	Technical Architecture for Information Management (TAFIM)
TBD	To Be Determined
TPFDD	Time Phased Force Deployment Data
TR	Test Report
TRR	Test Readiness Report
TS	Top Secret
UAT	User Acceptance Test
URP	User Review Panel
WAN	Wide Area Network
WWMCCS	World Wide Military Command and Control System

APPENDIX B

SYSTEM INTERFACES

This appendix describes the interfaces internal and external to GCCS. Since GCCS is a system of functions performed by many different applications that interact with many external systems and databases, it is necessary to clearly define the separation between internal and external interfaces. GCCS is defined to include within its boundaries those software items under the configuration management of DISA. GCCS includes all of the items that DISA owns, maintains, and updates for all GCCS sites.

INTERNAL INTERFACES

The GCCS Core database is the centerpiece of GCCS Version 2.1. and will be the first DoD CIM compliant, standardized database. Between GCCS sites, the Core databases communicate via the SIPRNET and ORACLE transactions. Within a GCCS 2.1 site, there are three ways that applications relate to the database. Some applications exclusively depend on the database for operation. Some applications require data from the Core database to be loaded into their own unique database for operation. The remaining applications do not use any data from the Core database.

DATABASE DEPENDENT

S&M, AHQ, PDR, IRM, RFA, RDA: These applications are each separate entities that do not interact directly with each other but directly access data in the Core database, update the database using SQL Plus, and create transactions which update the Core database through TDS. If the transactions are for networked OPLANS, the transactions will also be addressed and sent to other appropriate GCCS Core databases.

REQUIRE DATABASE DATA

JEPES, FAPES, JFAST, LOGSAFE, MEPES, IMRAS: These applications do not interact with each other except for MEPES and IMRAS. Each of these interact directly with LOGSAFE. These applications use IMS and RFM to obtain data from the Core database. IMS provides a means to move TPFDD data between the Core database and the application unique databases. IMS reads the TPFDD data from a Core resident OPLAN, converts it to the proper format, selects the appropriate data elements needed by the specific application, and loads the TPFDD data into the application. IMS can pickup TPFDD data from the file area of another application and move it back through the client/server communication to the Core database. The limitation of this approach is that the data will not be automatically distributed to other GCCS Core databases as would a transaction. RFM has 2 functions. One function, UPDATE retrieves the latest version of the reference file from the Core database into RFM. The other function, LOAD, copies the reference file from RFM into the application in the format required by the application.

DO NOT REQUIRE CORE DATABASE

GSORTS: It receives data sets for update into its ORACLE database from the NMCC. The AHQ can perform a query on this data through the Core database and use of SQL PLUS.

JMCIS, JDISS: They receive their data sets through SIPRNet and the internal addressing function. Neither of them interact with any other GCCS application.

EXTERNAL INTERFACES

The systems, data bases, or applications external to GCCS are grouped by those that interoperate via transactions, via send and receive message traffic, via receive only message traffic and via use of file transfer.

TRANSACTIONS

Army MOB/ODEE, Air Force COMPES, USTC GTN: These transmit transactions to and receive transactions from GCCS. The transactions are exchanged between the GCCS and the CINC/Service systems using Transaction Distribution Services (TDS) interface.

Army MOB/ODEE, receives transactions from GCCS that contain information on OPLAN forces (Army units) that FORSCOM must provide to the OPLAN. FORSCOM uses MOB/ODEE to update OPLANS with command approved data on active duty and reserve Army units. MOB/ODEE sends transactions to GCCS that provide detailed data on specific Army units that will support the OPLAN.

The Air Force COMPES provides a standard automated data system to capture, store, and report Air Force deployment operations, logistics and manpower data from the base level to the JCS. The OT&P part of COMPES provides a two-say transactional interface with GCCS to receive and update force requirements.

USTC GTN send Force and non-unit requirements updates as well as carriers with itinerary, allocations and manifests to the GCCS. The GTN/GCCS interface is at USTC.

SEND and RECEIVE MESSAGE TRAFFIC

AMHS, E-MAIL: These send and receive message traffic from CINC/Service systems. The GCCS capability is in the COE.

AMHS handles USMTF and DD-178/175 message formats. The source of the message can be any communications center.

E-Mail messages can have attached files in binary, ASCII or graphic formats. The message can be sent outside the GCCS domain provided it contains the domain address and is routed through the SIPRNet.

RECEIVE only MESSAGE TRAFFIC

JMCIS, JDISS, GSORTS: These operate in a "parent/child" receive only mode.

JMCIS can use USMTF or OTH-GOLD messages. The JMCIS parent in a CINC's headquarters receives information about the movement of vehicles, ships, planes, etc. The messages provide the "tracks" of movement for the reportable item. The tracks messages are received and written directly to the JMCIS parent database. JMCIS can forward all or selected tracks messages to child JMCIS databases for review.

JDISS uses USMTF messages. The JMCIS parent in a CINC's headquarters receives intelligence reports. The messages are accumulated into the parent database. The parent may forward all or selected messages to a child database for review on the child system.

GSORTS uses either message traffic or file transfer to move the GSORTS file from the NMCC to each GCCS site. Once at their site, the FDBM will use the GCCS RFA capability to move the GSORTS file into the Core database.

FILE TRANSFER

GCCS(T), Marine Corps MAGTF II, Navy RUDRS, DMA Map data, NMCC reference files:

GCCS(T) provides OPLANS, once they are downgraded to SECRET, to GCCS for further planning and execution.

The Marine Corps MAGTF II will download on OPLAN TPFDD that contains information on OPLAN forces (Marine units) for Marine Corps planner review sourcing. The planners will update the TPFDD with command approved data on active duty and reserve Marine units. The MAGTF II will produce a TPFDD file to update the OPLAN in GCCS.

Navy RUDRS permits the Navy to update OPLANS with command approved data on active duty and reserve Navy units. A GCCS OPLAN TPFDD download is accomplished and the file is transferred to RUDRS. Likewise, RUDRS produces a TPFDD file to update the OPLAN in GCCS.

Update files containing reference data needed to assist the warrior are transferred into GCCS from the DMA and NMCC using the File Transfer Protocol. The NMCC reference files transferred are: Geo-Locations, TUCHA, PORTS, APORTS, CHSTR, ASSETS, and LFF. Once at their sites, the FDBM uses the RFA to move the reference files into the Core database. The TUCHA and Geo-Locations data also can be updated by users at their host GCCS site using the new RFA capability. The RFA will produce a separate file of data updates in UNIX that can be file transferred to all other GCCS sites. The update files can be loaded to the Core database using ORACLE SQL. The movement of changed data must be coordinated with the JNOCC.

APPENDIX C

SUPPORTING DOCUMENTATION

GCCS Automated Information System (AIS) Security Plan for Version 2.0, May 1, 1995

GCCS Concept of Operation, DRAFT

Global Command and Control (GCC) Functional Economic Analysis (FEA), February 28, 1995

Global Command and Control System Exercise (GCCS-E), Exercise Positive Response 95-2, Draft Letter of Instruction (LOI), 7 April 1995

GCCS Evaluation Plan for GCCS Applications, October 7, 1993

GCCS Implementation Procedures for the GCCS Version 2.0, March 17, 1995

GCCS JOPES Database Implementation Strategy

GCCS Management Structure, CJCSI 6721.01

GCCS Mission Need Statement, June 8, 1995

GCCS Operational Evaluation Plan (OEP) Revision 2, May 1995

GCCS Program Management Plan, January 1995

GCCS System Administration Manual, May 12, 1995

GCCS Version Description Document for Version 2.1, June 15, 1995

JOPES Migration Assessment Plan, April 3, 1995

System Users Manual: GCCS Version 2.1, June 21, 1995

GCCS Version 3.0/3.1 EPIP, Annex C: Functional Description, May 30, 1997